TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2,00 €

n.147

HACKER JOURNAL

www.hackerjournal.it

WINDOWS XP



Alla **SCOPERTA** del SP3

MUSICA GRATIS

Last FM sempre con te

C++

PROGRAMMARE gli oggetti

WiFi

PROTEGGI la tua **CONNESSIONE WIRELESS**



LIBERO DI COMUNICARE

FREGA le intercettazioni e **BLINDA** i tuoi messaggi

Anno 8 – N.147
20 Marzo / 2 Aprile 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Chi trova **un amico...**

"Si può vivere senza fratelli, ma non senza amici."
Proverbio Arabo

Crescere, sempre!!! Questo è uno dei nostri motti e in questa ottica abbiamo deciso di lanciare una nuova "campagna acquisti" per usare un termine calcistico. A questo scopo abbiamo aperto una nuova casella di posta elettronica:

contributors@hackerjournal.it

chiunque voglia candidarsi a collaborare con noi è il benvenuto, chiunque pensi di poter contribuire alla stesura delle nostre pagine, chiunque abbia qualcosa di interessante da dire, chiunque condivida i nostri concetti di etica, libertà e hacking, chiunque abbia la voglia di insegnare agli altri quello che ha imparato.

Per evitare di perdere troppo tempo e tralasciare qualche proposta vi preghiamo di specificare nell'oggetto il tema di cui vorreste parlare (programming, p2p, linux, etc.) e di comunicarci anche la vostra età e i vostri contatti.

Confidiamo che sarete in molti a partecipare a questa iniziativa e vi preghiamo quindi di aver pazienza se non riusciremo a rispondere subito a tutti ma sappiate che leggeremo attentamente ogni mail.

Ovviamente, come ci sembra giusto, confidiamo nella massima correttezza etica di ciascuno di voi e siamo certi che non riceveremo articoli scopiazzati da internet o idee "rubate", insomma se volete far parte "dei nostri" sapete come dovete comportarvi!!!

Vi aspettiamo

The Guilty



HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

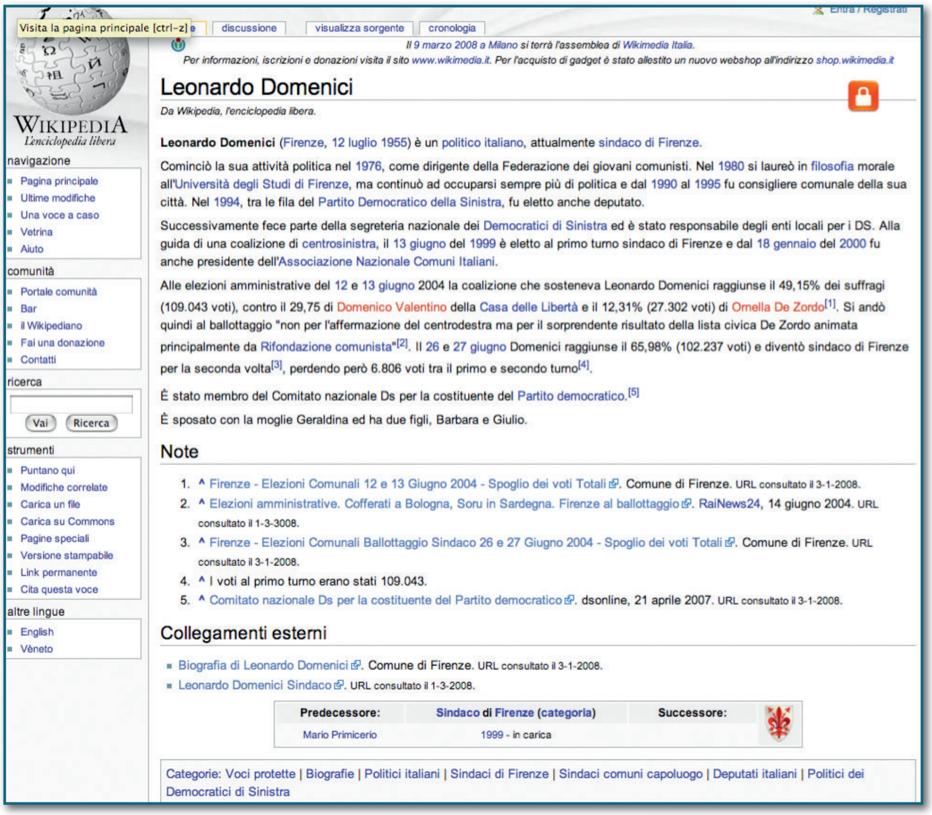
Wiki contro il sindaco

Non è la prima volta che succede, ma probabilmente la prima in Italia: Wikipedia, la più famosa enciclopedia on-line è stata denunciata dal sindaco di Firenze Leonardo Domenici e dall'assessore Graziano Cioni per diffamazione e calunnia. Cos'è successo??? Semplice, sulla voce di Wikipedia relativa al sindaco Domenici qualcuno ha aggiunto dati riguardanti un possibile illecito del sindaco e dell'assessore. Secondo le calunnie i due politici avrebbero assegnato ad una società esterna la gestione dei parcheggi, società che avrebbe nel proprio CDA le mogli degli stessi politici. Queste voci erano già girate e i due esponenti di DS avevano già proceduto ad una querela in proposito che ha portato ad una condanna e ad un rinvio a giudizio.

Il problema è sempre il solito in questo caso: Wikipedia è o no responsabile per quanto viene scritto nelle sue pagine??? Sappiamo che lo staff dell'enciclopedia non effettua nessun controllo preventivo sulle voci immesse e che proprio questo a portato ad una sua assoluzione non molto tempo fa in Francia. Il controllo delle voci è tutto affidato alla comunità che blocca, pulisce e censura (almeno così dovrebbe essere) i contenuti scorretti. Anche in questo caso il sistema ha funzionato ma solo a posteriori quando ormai la querela era partita. Ora la voce del sindaco è pulita e bloccata, non è più possibile modificarla, resta da capire se il giudice italiano si affiancherà a quello francese nel ritenere l'enciclopedia non responsabile dei suoi contenuti.

Di certo c'è che la possibilità di risalire all'autore della voce calunniosa è alta visto che la modifica risulta fatta dalla Biblioteca di documentazione pedagogica di Via Buonarroti a Firenze e se qui viene messa in atto la legge secondo cui gli utenti devono essere registrati sarà facile risalire al "calunniatore" che si troverà penalmente e civilmente responsabile per quanto scritto.

IngLS



Visita la pagina principale [ctrl-z] | discussione | visualizza sorgente | cronologia | Entra / Registrati

Il 9 marzo 2008 a Milano si terrà l'assemblea di Wikimedia Italia.
Per informazioni, iscrizioni e donazioni visita il sito www.wikimedia.it. Per l'acquisto di gadget è stato allestito un nuovo webshop all'indirizzo shop.wikimedia.it

WIKIPEDIA
L'enciclopedia libera

navigazione
- Pagina principale
- Ultime modifiche
- Una voce a caso
- Vetrina
- Aiuto

comunità
- Portale comunità
- Bar
- il Wikipediano
- Fai una donazione
- Contatti

ricerca
Vai | Ricerca

strumenti
- Puntano qui
- Modifiche correlate
- Carica un file
- Carica su Commons
- Pagine speciali
- Versione stampabile
- Link permanente
- Cita questa voce

altre lingue
- English
- Vèneto

Leonardo Domenici

Da Wikipedia, l'enciclopedia libera.

Leonardo Domenici (Firenze, 12 luglio 1955) è un politico italiano, attualmente sindaco di Firenze.

Cominciò la sua attività politica nel 1976, come dirigente della Federazione dei giovani comunisti. Nel 1980 si laureò in filosofia morale all'Università degli Studi di Firenze, ma continuò ad occuparsi sempre più di politica e dal 1990 al 1995 fu consigliere comunale della sua città. Nel 1994, tra le fila del Partito Democratico della Sinistra, fu eletto anche deputato.

Successivamente fece parte della segreteria nazionale dei Democratici di Sinistra ed è stato responsabile degli enti locali per i DS. Alla guida di una coalizione di centrosinistra, il 13 giugno del 1999 è eletto al primo turno sindaco di Firenze e dal 18 gennaio del 2000 fu anche presidente dell'Associazione Nazionale Comuni Italiani.

Alle elezioni amministrative del 12 e 13 giugno 2004 la coalizione che sosteneva Leonardo Domenici raggiunse il 49,15% dei suffragi (109.043 voti), contro il 29,75 di Domenico Valentino della Casa delle Libertà e il 12,31% (27.302 voti) di Ornella De Zordo[1]. Si andò quindi al ballottaggio "non per l'affermazione del centrodestra ma per il sorprendente risultato della lista civica De Zordo animata principalmente da Rifondazione comunista"[2]. Il 26 e 27 giugno Domenici raggiunse il 65,98% (102.237 voti) e diventò sindaco di Firenze per la seconda volta[3], perdendo però 6.806 voti tra il primo e secondo turno[4].

È stato membro del Comitato nazionale Ds per la costituente del Partito democratico.[5]

È sposato con la moglie Geraldina ed ha due figli, Barbara e Giulio.

Note

1. ^ Firenze - Elezioni Comunali 12 e 13 Giugno 2004 - Spoglio dei voti Totali. Comune di Firenze. URL consultato il 3-1-2008.
2. ^ Elezioni amministrative. Cofferati a Bologna, Soru in Sardegna. Firenze al ballottaggio. RaiNews24, 14 giugno 2004. URL consultato il 1-3-3008.
3. ^ Firenze - Elezioni Comunali Ballottaggio Sindaco 26 e 27 Giugno 2004 - Spoglio dei voti Totali. Comune di Firenze. URL consultato il 3-1-2008.
4. ^ I voti al primo turno erano stati 109.043.
5. ^ Comitato nazionale Ds per la costituente del Partito democratico. dsonline, 21 aprile 2007. URL consultato il 3-1-2008.

Collegamenti esterni

- Biografia di Leonardo Domenici. Comune di Firenze. URL consultato il 3-1-2008.
- Leonardo Domenici Sindaco. URL consultato il 1-3-2008.

Predecessore:	Sindaco di Firenze (categoria)	Successore:
Mario Primicerio	1999 - in carica	

Categorie: Voci protette | Biografie | Politici italiani | Sindaci di Firenze | Sindaci comuni capoluogo | Deputati italiani | Politici dei Democratici di Sinistra



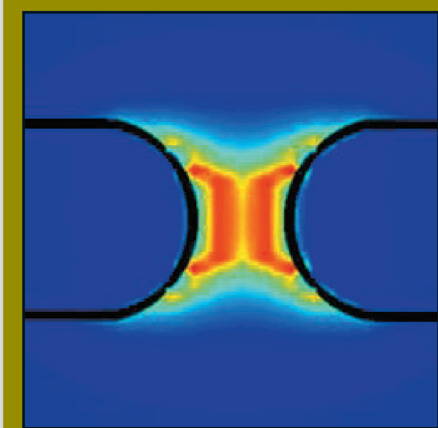


NUOVE DA ZIO BILL

Non si è ancora raffreddata la sua poltrona nell'ufficio di Redmond che zio Bill torna a parlare del mondo dell'informatica lanciando una previsione che lascia tutti... esattamente come prima!!! Il futuro dei computer è senza tastiera... Bella scoperta!!! Sappiamo tutti benissimo del progetto Surface di Microsoft e Apple si sta muovendo in questa direzione ormai da tempo, vedi iPhone e iPod Touch, tanto che prima della presentazione dell Mac Book Air si era parlato di un portatile copletamente touch con un sistema simile a quello dello smathphone di Cupertino.

VESTITI ELETTRICI

Si tratta della nuova frontiera della portabilità. Qual è difatti il più grosso problema di qualsiasi dispositivo mobile??? Ok, abbiamo pochi acces point wi-fi, ma nulla di non superabile, il vero limite al momento è la durata delle batterie, anche i nuovi prodotti come il Mac Book Air che vanta 5 ore di autonomia poi, alla prova dei fatti, in realtà dura solo 3 ore se stressato e questo con la batteria nuova... Quindi ben vengano idee come quella dei vestiti in grado di produrre energia con i movimenti del corpo. La cosa funziona tramite delle nanoantenne in grado di produrre energia elettrica partendo dall'atrito che si crea al contatto con l'aria o dalle vibrazioni. Queste nanoantenne sono sottili 100 volte di più che un capello umano e convertono l'energia meccanica in energia elettrica e possono produrre 80 mW per metro quadro di tessuto. Doviè la fregatura??? Beh, intanto tale tessuto non può essere lavato o le antenne andranno a farsi benedire ma gli esperti giurano che entro breve risolveranno anche questo problema e potremo alimentare il nostro cellulare semplicemente camminando.





TRADUTTORI DI VIRUS CERCASI

L'annuncio arriva dalla Russian Business Network, autrice dell'ormai famigerato Mpack, che sembra proprio essere alla ricerca di personale atto alla scrittura di codice (maligno ci viene da supporre) ma molto preparato anche sulle lingue in modo tale da finirla con le mail di phishing tradotte in maniera ridicola come ci capita tutti i giorni di ricevere sulla nostra casella. Insomma, un po' di professionalità anche nelle frodi!!!!

TROJAN PER WINDOWS MOBILE

Difficile trovare virus per dispositivi mobili, soprattutto per Pocket Pc e Windows Mobile visto la loro scarsa diffusione ma a quanto pare qualcuno ha deciso di interrompere il digiuno e ha lanciato InfoJack. Si tratta di un trojan vecchio stile che si installa e invia alla case madre notizie sulla device dove si trova (sistema operativo, numero di serie e altro). Di buono c'è che non si autoinvia ad altri utenti ma rende il dispositivo assolutamente disarmato verso altri ulteriori attacchi. Il sito verso cui puntata il virus è ora stato chiuso.





HOT NEWS

BUTTA VIA TUTTO!!!

Questo è il grido di allarme che lancia un nuovo virus che circola in rete. Si tratta di un falso messaggio di allarme che ti arriva dicendo che stanno indagando su di te e che quindi ti conviene cancellare i tuoi file "scottanti", il tuo nome sarebbe compreso in una lista di 150 persone inquisite che puoi visionare cliccando sul link... E qui c'è la fregatura... Il webserver ha cui il virus fa riferimento è nell'Illinois (USA) e si sta procedendo alla sua chiusura.



CHE NOIA!!!

Siamo quasi stufi di riferire di buchi di sicurezza in siti di social networking... Questa volta incriminati sono Yahoo! Messanger, MySpace e Facebook e il baco sarebbe relativo i controlli ActiveX. Secondo i ricercatori che hanno scoperto la falla questa potrebbe addirittura portare a sovrapporsi alla memoria tampone bloccando il sistema, unico rimedio bloccare ActiveX fino a relativa patch che coprisse il buco.



Viaggi online?

Nel panorama dei siti per la prenotazione di aerei, auto, alberghi e altro per i viaggi è nato un nuovo sito chiamato www.momondo.com. Oltre ai classici motori di ricerca per voli, alberghi e auto si può trovare una buona sezione di articoli, ovviamente a fondo "turistico" e una sezione chiamata share e impostata in termini di socialnetworking. Da tenere presente nell'organizzare il nostro prossimo viaggio.

TRANSIT IL PULMAN DI GOOGLE

Un nuovo servizio è da poco presente all'interno di Google Maps, si chiama Transit e fornisce agli utenti indicazioni su come pianificare un tragitto utilizzando i mezzi pubblici. Con un semplice clic, il servizio segnala all'utente le tratte coperte, le fermate più vicine al punto di partenza e di destinazione, i tempi di percorrenza e persino gli orari di riferimento, direttamente sullo schermo. Caratteristica principale di Google Transit è la possibilità di costruirsi ad hoc un percorso che preveda l'utilizzo di diversi mezzi: tram, autobus, metropolitana, treno. Per il momento il servizio copre solo la provincia di Firenze e Torino ma sono già in previsione accordi con le altre reti e quindi una maggiore copertura.



GMAIL BUCATA

Gli utenti della posta di Google in Kuwait hanno avuto non pochi problemi di sicurezza. Secondo alcuni utenti infatti per alcuni giorni era quasi impossibile accedere ai propri account mentre risultavano visibili le informazioni di altre persone iscritte al servizio. La colpa sarebbe di un Isp kuwaitiano che avrebbe avuto problemi di cache mandando in tilt il sistema di log-in. Sembra che gli stessi problemi abbiano investito anche eBay ma la notizia non è confermata.

BitTorrent su iPhone



Sarebbe già pronto e funzionante il primo client di Torrent per lo smartphone made in Cupertino. Per ora si tratta ancora di un beta e lo sviluppatore consiglia di non utilizzare il client tramite connesseione EDGE ma solo via Wi-Fi, pena far crollare la connessione per eccesso di traffico.

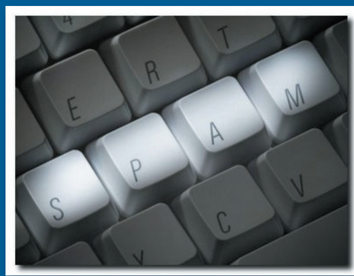


CINA VS. AMATOURS

Continua ad aumentare il numero di individui arrestati dalle autorità cinesi in seguito alla diffusione, non autorizzata, di alcune immagini hard di una celebrità di Hong Kong, l'attore e cantante Edison Chen. Due nuove persone si sono aggiunte alle 5 già condannate per aver trafugato da un portatile dell'attore, mandato a riparare, delle foto hard dello stesso e poi averle diffuse in rete.

AL GABBIO LO SPAMMATORE

La Corte Suprema della Virginia, negli Stati Uniti, a condannato a nove anni di carcere Jeremy Jaynes, accusato di aver mandato milioni di messaggi di posta indesiderata ad altrettanti ignari utenti internet. Una sentenza che, sicuramente, entrerà nella storia della Rete. La vicenda, tra ricorsi e carte bollate, va avanti già dal 2003, anno del primo arresto di Jaynes. L'accusa ha presentato la prova di 53mila messaggi e-mail illegali inviati in soli tre giorni, ma tra luglio e agosto del 2003 pare che l'uomo abbia mandato un milione di messaggi spam al giorno. La difesa, invece, ha basato le sue argomentazioni sul fatto che le leggi anti-spam emanate ultimamente negli Stati Uniti violerebbero i diritti del primo emendamento della Costituzione degli Stati Uniti, quando si tratta di anonimato.



METTI UN COBRA NEL MOTORE

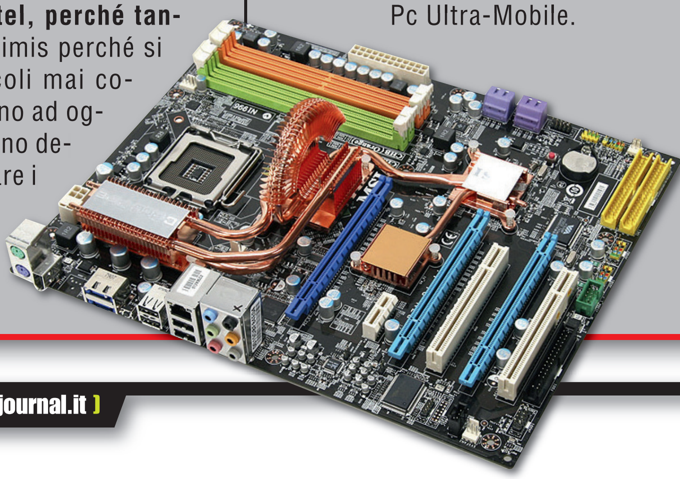
Si chiama Cobra e si propone come nuovo linguaggio di programmazione open source utilizzabile per scrivere applicazioni sulla piattaforma MS.NET o su Mono. Il linguaggio non è nuovo, esiste infatti da due anni, ma solo ora il suo creatore ha rilasciato il codice sorgente sponsorizzando il suo linguaggio come la sintensi dei pregi di Python, Ruby, Smalltalk, Boo, OBjective-C, C++ e Java.



INTEL ATOM-ICO



Si chiameranno Atom i nuovi processori di casa Intel, perché tanto interesse, in primis perché si tratta dei più piccoli mai costruiti dalla casa fino ad oggi e sembra che siano destinati a equipaggiare i nuovi sistemi portatili anche grazie alla bassissima richiesta energetica che hanno. I processori al momento sono due Silverthorne e Diamondville, il primo dedicato alle Mobile Internet Device mentre il secondo ai Pc Ultra-Mobile.



L'architettura dei processori è completamente nuova e per certi versi più semplice dei Core ma con tecnologie assolutamente all'avanguardia come il supporto multi-threading e il Deep Power Down.

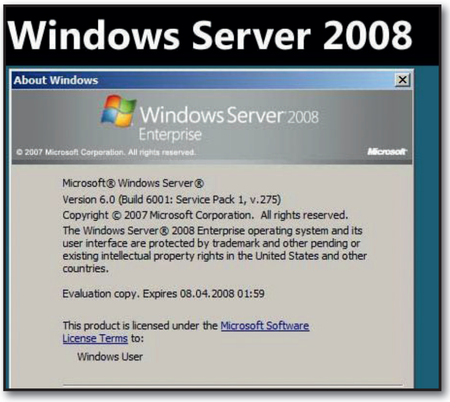




HOT NEWS

WINDOWS SERVER 2008

Non parleremo dell'ennesima multa comminata a Microsoft per abuso di posizione dominante ma bensì del nuovo os per server basato sul database Sql 2008 e sulla suite Visual Studio 2008. Scopo non troppo celato togliere mercato ai serve Linux based spesso preferiti per questioni di sicurezza e costi.



A SPASSO SULLA LUNA

Sembra che sarà italiano il primo robot privato che muoverà i suoi passi sulla luna. Il progetto si chiama AMALIA e concorre al Google Lunar X Prize. Si tratta di una iniziativa lanciata dal motore di ricerca che ha messo in palio 30 milioni di dollari per il primo dei dieci gruppi privati partecipanti che arriverà con la propria sonda motorizzata sulla Luna.



ISO0 OOXML

Non ci siamo drogati e digitiamo tasti a caso ma stiamo parlando della possibilità che Office Open XML di Microsoft entri a far parte della comunità dei formati aperti. Già l'anno scorso ci avevano provato incassando una bocciatura, quest'anno le voci sono discordanti ma ci sarà bisogno di tutta la forza di Redmond per arrivare ad un esito positivo.

FOTO HD

Ormai l'HD spopola e mancavano giusto le foto, ora il buco è stato coperto dalle Lumix di Panazoni con la predisposizione per la funzione HD Photo che permette di memorizzare le foto in formato 1.920x1.080 per poterle rivedere immediatamente sul nostro schermo HD.





STEVEN E I GIOCHI

Il famoso regista Steven Spielberg ha deciso di entrare a gamba tesa nel mercato dei videogiochi con un nuovo progetto che per ora ha il misterioso nome di Lmno. Il concetto di base è diu creare un rapporto emozionale con il giocatore, Spielberg vuole farci piangere e ha dichiarato che il gioco sarà "come se Intrigo Internazionale di Hitchcock incontrasse E.T.", non male come prospettiva. Non si hanno ancora date di rilascio ma sembra sicuro che il gioco girerà sia su PS3 che su Xbox 360.



last.fm ovunque

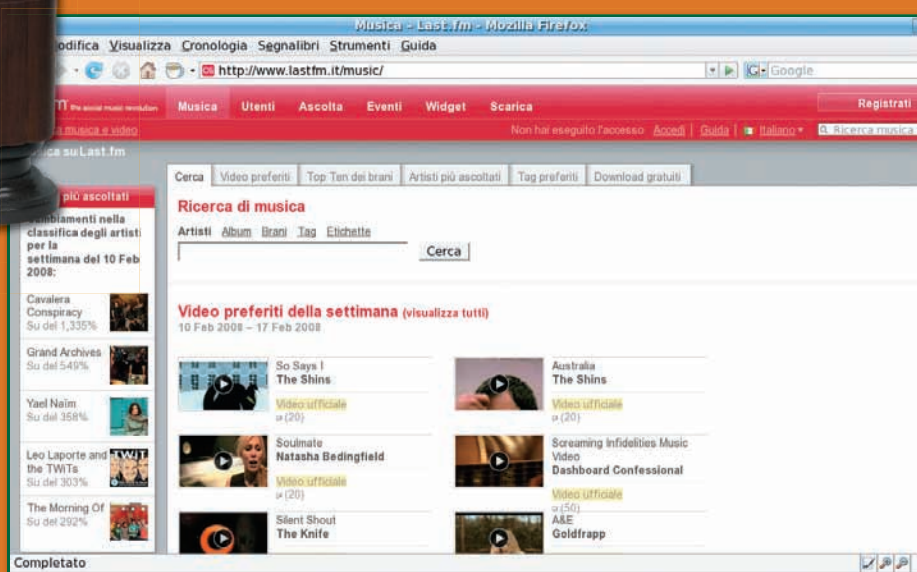


Con un proxy possiamo usare il nostro lettore audio preferito per ascoltare la musica da Last.fm... e possiamo anche scaricare i brani su hard disk

Last.fm è un'eccellente radio online, ricca di buona musica e con una vivacissima comunità di utenti alla base. Sintonizzarci sulle sue stazioni, insomma, è un vero piacere, qualsiasi sia il nostro genere musicale d'elezione; il lettore audio ufficiale di Last.fm, però, può non incontrare i gusti di tutti gli utenti. Perché non scegliere direttamente noi il player con cui sintonizzarci? In queste due pagine, dunque, faremo la conoscenza di LastFMProxy, un proxy server da installare sul PC che ci consentirà di "dirottare" la musica di Last.fm su di un player audio a nostra scelta. Oltre a questa sua funzionalità principale, LastFMProxy ci permetterà anche di salvare su hard disk i brani che ascolteremo via via dalla radio online.

:: Installiamo LastFMProxy

Il programma LastFMProxy funziona su Linux, Windows e Mac OS X; in queste prove verrà utilizzato Linux come sistema operativo. Andiamo sul sito di LastFMProxy, http://vidar.gimp.org/lastfmproxy/, e scarichiamo l'ultima versione del programma (attualmente è la release 1.3b).

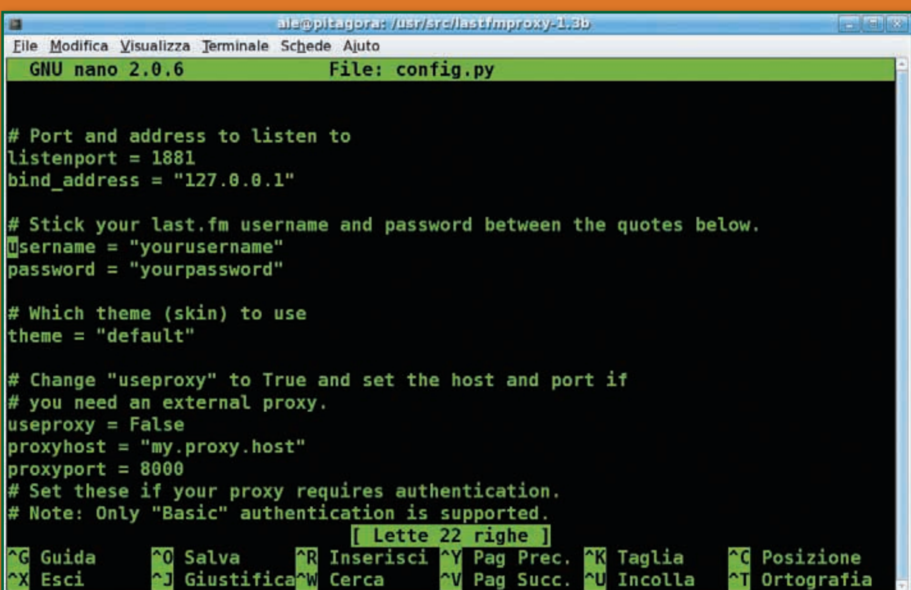


▲ *Il sito di Last.fm. Tutti i generi per tutti i gusti musicali: finalmente la radio la facciamo noi!*

Apriamo una console, entriamo nella directory in cui abbiamo salvato il file e scompattiamo l'archivio con "tar xvfz lastfmproxy-1.3b.tar.gz"; entriamo nella cartella appena creata ("cd lastfmproxy-1.3b/") ed apriamo il file config.py con il nostro editor preferito.
Modificando questo file adatteremo la configurazione di LastFMProxy al nostro sistema. Le righe fondamentali da cambiare in config.py sono quelle che permettono a LastFMProxy di avere accesso al nostro utente su Last.fm: inseriamo nella linea 'username = "yourusername"' il nome del nostro utente e in 'password = "yourpassword"' la password relativa.

:: Configurazione avanzata

LastFMProxy utilizza come porta di default la 1881. Nel caso questa fosse occupata da un altro servizio, cambiamola nella riga "listenport = 1881 ". Per ragioni di sicurezza il proxy risponde esclusivamente sulla macchina locale (localhost); se vogliamo aprire il proxy al mondo esterno modifichiamo la linea 'bind_address = "127.0.0.1"' in 'bind_address = "0.0.0.0"' (l'indirizzo 0.0.0.0 metterà il proxy in ascolto su tutte le interfacce disponibili). Effettuate le modifiche necessarie, salviamo il file e chiudiamo l'editor.

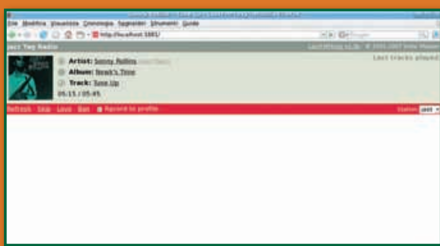


Per poter usare LastFMProxy basta inserire nella configurazione il nome utente e la password di accesso.

A questo punto possiamo lanciare il proxy con il comando "./main.py &", sempre restando all'interno della directory lastfmproxy-1.3b.

:: Sintonizziamoci!

Una volta avviato il proxy, sinceriamoci che questo funzioni correttamente. Apriamo il nostro web browser e facciamolo puntare all'indirizzo http://localhost:1881/. Comparirà una spartana ma completa interfaccia web per Last.fm: clickiamo sul pulsante "Start radio" per far partire il player multimediale di default nel web browser ed ascoltare così la musica dalla radio online. Per cambiare "stazione" modifichiamo, semplicemente, l'indirizzo a cui puntare: scrivendo http://localhost:1881/lastfm://globaltags/jazz, ad esempio, sceglieremo 'jazz' come tag d'ascolto.



L'interfaccia web di LastFMProxy.

::Last.fm con un player qualsiasi

Ora possiamo far dialogare il nostro player multimediale preferito con LastFMProxy: configuriamo il web browser per richiamare in automatico il nostro lettore quando si aprono dei file MP3 in streaming (sono i file con estensione .m3u). In questo modo il player multimediale verrà avviato appena clickeremo sul pulsante "Start radio" nell'interfaccia web di LastFMProxy. Oltre a questo, possiamo anche ascoltare direttamente le stazioni tramite un player: ci basterà fornire a questo l'indirizzo del file .m3u su cui "sintonizzarci", ad esempio http://localhost:1881/globaltags/classical.m3u per sintonizzarci sul tag 'classical'. Il player dovrà avere una funzione per l'ascolto delle playlist; per collegarci al proxy Last.fm da mplayer, dunque, utilizzeremo una linea del tipo "mplayer -playlist http://localhost:1881/globaltags/classical.m3u", mentre se usiamo VLC ci basterà richiamare nella linea di comando l'indirizzo del file .m3u, senza opzioni aggiuntive.

::Salviamo la musica sull'hard disk

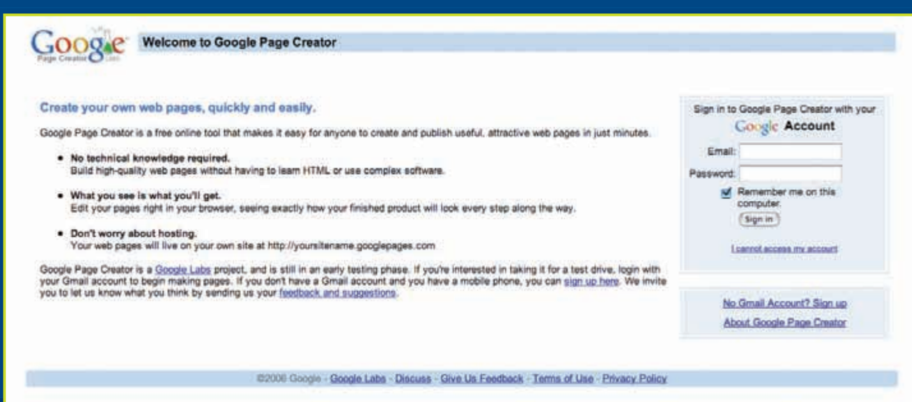
Dopo tutta questa ubriacatura di musica in streaming c'è venuta voglia di scaricare qualche brano sul PC? Quello che ci serve è Streamripper. Preleviamo da http://streamripper.sourceforge.net l'ultima versione del programma, scompattiamo il pacchetto con "tar xvfz streamripper-1.63-beta-4.tar.gz" ed entriamo nella directory streamripper-1.63-beta-4; per compilare ed installare il software diamo la consueta sequenza di comandi "./configure; make; make install" da root.
Ora non ci resta che collegare streamripper al proxy Last.fm sul nostro PC: il programma scaricherà i vari brani che verranno suonati dalla stazione su cui siamo sintonizzati, inserendo artista e nome corretti nei nomi dei file mp3 salvati. Sintonizziamoci con un lettore qualsiasi sulla nostra stazione Last.fm preferita, quindi chiudiamo il lettore ed in una console eseguiamo "streamripper http://localhost:1881/lastfm.mp3". Quando ci siamo stancati di salvare la musica sull'hard disk entriamo nella console e schiacciamo Ctrl+C. ■

Chi cerca trova... IL MALWARE



Si pensa che non comporti nessun rischio invece basta aprire Google ed effettuare una ricerca per essere esposti

A volte quando navighiamo su Internet, anche solo per cercare la biografia del nostro attore preferito, abbiamo l'impressione di essere un Marine in una giungla che pullula di Vietcong, pronti a piantarci una pallottola in testa. Adesso non possiamo neanche più stare tranquilli su Google. Dopotutto, il più importante motore di ricerca del mondo non poteva venire ignorato da quei delinquenti che non hanno niente di meglio da fare che riempire di immondizia il Web. Anzi, sembra proprio che il nostro amato portalone sia uno dei mezzi più efficaci per spargere ogni sorta di codice maligno e poiché i cybercriminali hanno molta fantasia i modi escogitati per renderci la navigazione meno piacevole sono sempre più subdoli. Per esempio, si è scoperto che, grazie a specifici interventi sul SEO (Search Engine Optimization), cioè il motore che ottimizza i risultati delle ricerche, riuscivano a mettere in cima all'elenco dei risultati ottenuti i loro siti infestati da virus. Bastava quindi un clic e l'ignaro utente veniva spedito in una di queste pagine, pronte a imbottirgli il computer di ogni genere di schifezza informatica. Per fortuna, gli angeli custodi di Google se ne sono accorti e sono corsi ai ripari, ma ovviamente qualche danno era già stato fatto.



Un altro sistema molto efficace per danneggiarci è stato inventato per aggirare i filtri antispam, nonostante questi diventino di giorno in giorno sempre più efficienti e difficili da prendere per il naso. In questo caso bastava inserire il codice maligno in un sito ritenuto sicuro per spedire la vittima dove si voleva. È proprio quello che è successo con Google Page Creator, la pagina che ci aiuta a creare i nostri siti Web.

A questo punto viene proprio da dubitare che chi ha l'incarico di vigilare sulla nostra sicurezza stia davvero facendo del suo meglio.
Maliziosamente ci chiediamo, com'è possibile che dei cani sciolti riescano a mettere in crisi i sistemi di aziende multimiliardarie?

O più semplicemente non siamo di fronte a dei cani sciolti?

Il WEB e la tutela dei MINORI

Parola d'ordine vegliare!!! Come ogni strumento messo in mano ad un bambino anche un pc può essere fonte di cerescita o di pericoli

In queste pagine abbiamo sempre sostenuto che il primo vero baluardo di difesa contro le minacce di Internet è il nostro comportamento... e continuiamo a sostenerlo. Il nostro computer viene però sempre più spesso usato anche dai bambini, che sono infaticabili navigatori della Rete... a volte anche piuttosto sconsiderati! Ci fa davvero pensare una ricerca condotta da Dafna Lemish dell'Università di Tel Aviv (Israele), che mette in evidenza quanto poco sappiano i genitori del comportamento in Rete dei loro figli. Siccome in questo caso è più che mai vero il proverbio "Tutto il mondo è paese", cerchiamo di capire meglio cosa fanno i nostri ragazzi... magari sotto il nostro naso.

Dal campione di 500 giovani tra i 9 e i 18 anni è emerso che parlare con sconosciuti e imbattersi in materiale pornografico sono quasi delle normalità. Ma la cosa inquietante è che il tutto avviene all'insaputa dei genitori, spesso assenti durante i collegamenti. Il 73% ammette candidamente di comunicare dati strettamente personali, come l'indirizzo e il numero di telefono. Inoltre, il 36% sostiene di cercare incontri con persone conosciute in Internet. Inutile sottolineare il pericolo che tutto questo implica! Naturalmente i nostri figli sono svegli, quindi sanno bene come cancellare le tracce della loro navigazione e tenerci fuori da quelle che ritengono loro faccende private. Più che a un disinteresse, la Lemish imputa tutto questo a una fondamentale ignoranza da parte delle famiglie dei pericoli che si nascondono sul Web. Naturalmente è possibile tutelare i minori e la nostra privacy.



Se proprio non abbiamo tempo di navigare insieme a loro, possiamo adottare i programmi per il controllo parentale. In pratica, si tratta di filtri personalizzabili in base all'età dei figli, per impedire loro di collegarsi a nostra insaputa a siti "proibiti", o svolgere attività potenzialmente pericolose. Normalmente si tratta di software abbastanza facili da usare e ce ne sono molti anche in italiano. È però necessario aggiungere che queste applicazioni possono solo aiutarci a tutelare i nostri figli, ma non possono sostituirsi completamente a noi. ■



La RETE sotto chiave

Scopriamo come nascondere la rete wireless da occhi indiscreti con Vista

Sempre più spesso in casa e in ufficio i nostri computer sono collegati tra loro e con Internet attraverso le reti senza fili basate sulle specifiche Wi-Fi. Comodissime, lo sono ancora di più se abbiamo installato Windows Vista.

Il sistema operativo di Microsoft dispone infatti di efficaci strumenti che consentono di rilevare e gestire una rete wireless con pochi clic del mouse. Dobbiamo però fare attenzione ai "pirati" che tentano di collegarsi senza permesso alla nostra rete, un'eventualità tutt'altro che remota soprattutto se abitiamo ai piani bassi o in un affollato condominio. In sostanza, è necessario prendere le dovute contromisure, come illustreremo nelle prossime pagine.

::Cacciamo i curiosi

Le reti senza fili consentono di collegarsi a Internet e di sfruttare le risorse condivise dei nostri computer da qualunque punto della nostra casa. Se ci spostiamo dal salotto alla cucina, non c'è neppure bisogno di interrompere una sessione di chat o la lettura di una pagina Web. Ma a che serve tutta questa

versatilità se poi basta un computer dotato di adattatore Wi-Fi per penetrare nelle nostre difese? È dunque di fondamentale importanza rendere difficile la vita ai malintenzionati. Ma quanto alte devono essere le "barriere protettive"?

Conviene davvero "blindare" il nostro sistema impostando i massimi livelli di sicurezza per poi vedere trasformato l'accesso alla rete in una continua richiesta di autorizzazioni e conferme?

COSA SIGNIFICA?

DHCP
Dynamic Host Configuration Protocol Sistema che permette di attribuire automaticamente a qualunque dispositivo collegato alla rete (PC, server, stampanti...) un indirizzo univoco per identificarlo.

MAC Address
Indirizzo MAC
Identificativo unico di ogni dispositivo di rete, non solo senza fili, costituito da una serie di lettere e numeri.

WEP
Wired Equivalent Privacy
È il principale strumento di difesa delle reti basate sullo standard 802.11. In sostanza si tratta di una sorta di password da impostare sia sul punto di accesso (o sul router) sia sulle schede wireless affinchè possano liberamente -ma in sicurezza- comunicare tra loro. Purtroppo, per scalcare il WEP bastano un portatile con Wi-Fi e un piccolo programma scaricabile dal Web.

WPA
Wi-Fi Protected Access
Il sistema di sicurezza WEP si è dimostrato nel tempo troppo vulnerabile. Per questo è stato rimpiazzato dal più affidabile WPA, molto più sicuro del suo predecessore, soprattutto nella versione WPA2.

:: Il giusto compromesso

Eliminare tutte le richieste di password e tutte le protezioni della nostra rete senza fili è certamente la mossa peggiore che potremmo fare. Viceversa, un sistema iperprotetto rischia di diventare inutilizzabile. Vista ci mette a disposizione un bel po' di opzioni che se ben impostate ci mettono al sicuro senza troppi grattacapi. Nel peggiore dei casi, sono richiesti un paio di passaggi in più per stabilire la prima connessione alla rete wireless. Il primo accorgimento è quello di inserire una chiave per "crittografare" i dati trasmessi. Esistono diversi tipi di crittografia, ma se tutti i nostri computer usano Windows Vista scegliamo senza indugio la protezione WPA, più affidabile della vecchia WEP. In questo modo la nostra rete senza fili richiederà una password di accesso a tutti i tentativi di connessione e tutte le trasmissioni saranno "nascoste" da occhi indiscreti e quindi sicure.

:: L'indirizzo è sbagliato

Una delle caratteristiche meno usate ma efficaci nella protezione delle nostra rete senza fili è il blocco degli accessi sulla base del MAC Address della scheda di rete. Ogni MAC Address è un indirizzo fisico univoco al quale corrisponde una e una sola scheda di rete senza fili: quest'ultima, in pratica, è individuabile indipendentemente dal sistema operativo o dagli altri parametri di connessione. La maggior parte dei router senza fili permette di filtrare il traffico sulla base di questo indirizzo. La soluzione più rapida è quindi consentire l'accesso solo agli indirizzi MAC dei nostri computer.

:: Top secret

Praticamente qualsiasi router wireless, nella configurazione di base, rende visibile a tutti il nome della rete senza fili, in modo da consentire un accesso più facile: chiunque può trovare la rete e tentare l'accesso.

LA CHIAVE WPA

Il primo passo da fare dopo aver cambiato il SSID del nostro router, è quello di impostare una chiave WPA.

Passo 1
Il menu "opzioni"
Nella maggior parte dei router, le opzioni di sicurezza che ci interessano sono in una sezione chiamata Wireless. Cerchiamo una voce chiamata I WPA Pre-Shared Key, oppure WPA-PSK.



Passo 2
Scegliamo una password
Inventiamo una password lunga e articolata, con lettere e numeri quindi inseriamola nella casella. Conserviamo questa password in un posto sicuro: ci servirà ogni volta che collegheremo un nuovo PC wireless alla rete senza fili.

È possibile personalizzare come preferiamo il nome della nostra rete, cioè il SSID, inoltre si può anche impostare un SSID nascosto. Così facendo, potrà accedere manualmente alla rete senza fili solo chi ha tutti i dati, compreso il nome SSID che abbiamo assegnato.

:: Bando al DHCP

Se temiamo gli attacchi dall'esterno, un'altra opzione che dobbiamo prendere in considerazione è quella di impedire al router wireless di fornire il servizio DHCP. Se questo servizio è attivo, infatti, qualunque computer collegato riceve in automatico le impostazioni necessarie per accedere a Internet e alle risorse condivise della rete locale.

Se disattiviamo il DHCP dobbiamo assegnare un IP fisso a tutti i computer: poco male se i PC che usiamo sono sempre gli stessi, mentre qualche problema può nascere quando arriva un amico e vuole collegarsi alla nostra rete con il proprio portatile. In aggiunta bisogna tenere presente che se il router wireless è collegato a un modem ADSL, spesso il servizio DHCP è delegato a quest'ultimo.

BLOCCA IL MAC ADDRESS

Il passo successivo è quello di impostare i sistemi di sicurezza basati sugli indirizzi MAC dei nostri dispositivi di rete. È abbastanza semplice. Ecco come fare

Passo 1
Scopriamo il nostro indirizzo MAC
Dobbiamo scoprire il MAC Address della nostra scheda di rete. Apriamo il Centro connessioni di rete e condivisione di Vista: dalla rete wireless, scegliamo Visualizza stato I e Dettagli.

Passo 2
Scrivilo su un foglio
Nella finestra che si apre, cerchiamo la voce Indirizzo fisico. Si tratta di una serie di cifre esadecimali. Annotiamole da qualche parte, lontano da occhi indiscreti. Possiamo ora chiudere tutto e dedicarci al router.

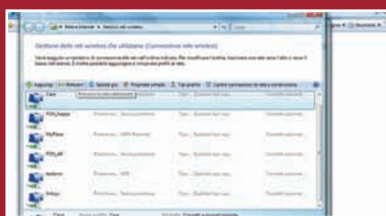
Passo 3
Abilitiamo il filtro MAC
Nel pannello del router I cerchiamo la voce Mac Filtering o Wireless Mac Filtering. Abilitiamola e specifichiamo che vogliamo permettere l'accesso solo ai PC elencati nella lista che stiamo per creare.

Passo 4
Selezione all'ingresso!
Inseriamo nella lista l'indirizzo o gli indirizzi MAC del PC a cui concedere l'accesso. Alcuni router richiedono che le coppie di numeri siano separate dai due punti.

ACCEDO ALLA RETE WIFI

Ora che la rete senza fili è blindata, possiamo procedere con il collegamento del nostro computer. Grazie alla procedura guidata di Windows Vista, questa operazione è estremamente rapida: basta seguire i passi proposti e inserire i dati che di volta in volta ci vengono richiesti.

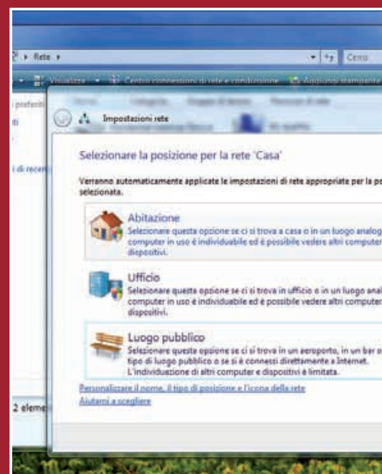
Passo 1
Cancelliamo tutti i profili
Facciamo clic con il tasto destro del mouse sull'icona delle reti nella barra delle applicazioni di Vista e scegliamo Gestisci reti wireless. Eliminiamo tutte le vecchie impostazioni con il pulsante Rimuovi.



Passo 2
Ritroviamo la nostra rete
Con un altro clic destro sull'icona delle reti di Vista, scegliamo di collegarci alla nostra rete. Se abbiamo nascosto il SSID, scegli la connessione manuale e specifichiamone ora il nome.

Passo 3
Ci vuole la password!
Dopo qualche secondo, Windows Vista ci richiede la password per la connessione. Inseriamo quella che abbiamo precedentemente impostato nel router alla voce WPA, quindi premiamo il pulsante Connetti.

Passo 4
Tutto automatico
Attendiamo che Windows Vista ci comunichi il risultato della connessione. Se è andato tutto bene, ci proporrà di salvare la rete per i futuri accessi automatici. Non dovremo così ogni volta ripetere l'operazione. Accettiamo e portiamo a termine la procedura.



Passo 5
Dove siamo?
Dopo esserci collegati, Vista ci chiede di che tipo di rete si tratta. Ora che è sicura, scegliamo Abitazione in modo da abilitare tutte le condivisioni da e verso I gli altri PC della rete.

Passo 6
Controlliamo il riepilogo
L'ultima schermata ci informa sulle modalità di connessione e su quello che la rete farà. Se vogliamo, possiamo modificare le impostazioni manualmente nel Centro connessioni di rete e condivisione.

:: Tutto utile

Grazie agli accorgimenti mostrati in queste pagine, possiamo rendere la nostra rete senza fili molto più sicura. Se temiamo che la gestione della rete finisca col diventare troppo impegnativa, non ci dobbiamo preoccupare: basta annotare il nome della rete e la password con cura, dopodiché Vista ci guiderà nella configurazione dell'accesso senza la minima difficoltà. Anche l'inserimento di un nuovo computer non è un dramma: è sufficiente ricordarsi di inserire il MAC Address della nuova macchina nella lista degli indirizzi presente nelle opzioni del router.

ENLARGE YOUR...URL.

Quando le dimensioni contano

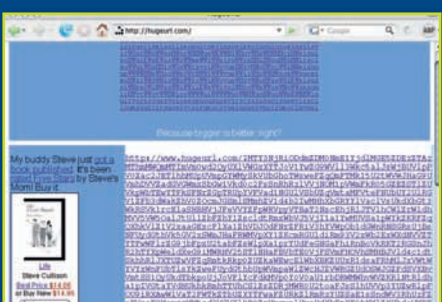
Tutti usano i servizi di abbreviazione degli url? E allora distinguetevi con un indirizzo web lungo, anzi lunghissimo

TinyUrl, ElfUrl, SnipUrl, Urlsaw, TightUrl, url(x), Shorl, SHurl e ElfUrl: questi sono solo alcuni dei servizi che abbiamo visto in Hacker Journal 114 per accorciare a lunghezze gestibili gli indirizzi lunghi di forum, newsgroup o pagine molto annidate di un sito. In particolare TinyUrl è ormai molto conosciuto perché usato in automatico da alcuni servizi dove la brevità è d'obbligo, ad esempio su Twitter in cui si ha a disposizione all'incirca lo spazio di un SMS e un indirizzo lungo ruba spazio a ciò che vogliamo dire.

:: Lunghissimo è bello

C'è però chi ama andare controcorrente e fornire un'alternativa, che magari prende in giro tutta questa improvvisa mania di brevità.

In nostro aiuto vengono in aiuto i tipi di HugeURL (http://hugeurl.com/) il cui motto è



Questo è il risultato dell'allungamento di www.hackerjournal.it

"Because bigger is better, right?" e cioè "più grosso è meglio, giusto?". Giusto! Grazie a HugeURL possiamo trasformare qualsiasi indirizzo in una mostruosità che occupa un'intera schermata. Ad esempio il semplice www.hackerjournal.it diventa un url incomprensibile di quasi trenta righe lungo 1500 caratteri pseudocasuali: lungo, difficile da leggere, ricordare e gestire e senza alcun indizio su dove ci porterà. Viene quasi voglia di farci una t-shirt.

:: Fate la vostra scelta

Stessa idea, stesso nome ma approccio diverso è quello di HugeURL (http://hugeurl.wiggy.net/) che addirittura ci offre la scelta su vari modi in cui può allungare ed ingarbugliare i nostri indirizzi.

Il risultato sarà sempre un indirizzo del tipo http://hugeurl.wiggy.net/go/qualcosa



C'è davvero l'imbarazzo della scelta e possiamo decidere di codificare in puro stile geek usando il base64, l'MD5 (usato per l'hashing) o l'UUID. Oppure optare per lo scrambling, che cambia le lettere, il verboso TLA o ancora la traduzione in "Swedish chef", il finto svedese in cui parla uno dei Muppets.

:: Enlarge your mailbox

Se poi volete davvero strafare oltre che le pagine web c'è anche modo di rendere assurdamente lungo anche il vostro indirizzo di posta elettronica. Esiste infatti un provider che offre caselle e-mail gratis sul dominio abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijk.com

No, non è uno scherzo! Anzi, sì è uno scherzo ma si fa sul serio: andando sul sito http://abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijk.com/ si può ottenere una webmail con la capienza ridicola di 6 MB che vi assicura l'indirizzo alfabetico più lungo che esista e promette divertimenti (leggi: problemi) a non finire. Un indirizzo così lungo non se lo ricorderà nessuno (nemmeno il sito stesso) o non verrà ritenuto reale ma può venire rifiutato anche dai computer stessi, ad esempio quando inserito nei form online, o nella configurazione del vostro client di posta.

Nicola D'Agostino

BLINDA le tue COMUNICAZIONI

Internet e cellulari hanno cambiato il nostro modo di comunicare, ma offrono ai malintenzionati ghiotte occasioni per intromettersi nella nostra privacy. Impariamo a difenderci



Ogni giorno facciamo telefonate con il nostro cellulare, spediamo decine di email e comunichiamo tramite programmi come MSN Messenger o ICQ. Miliardi di informazioni che viaggiano in Rete e che possono essere intercettate facilmente da malintenzionati.

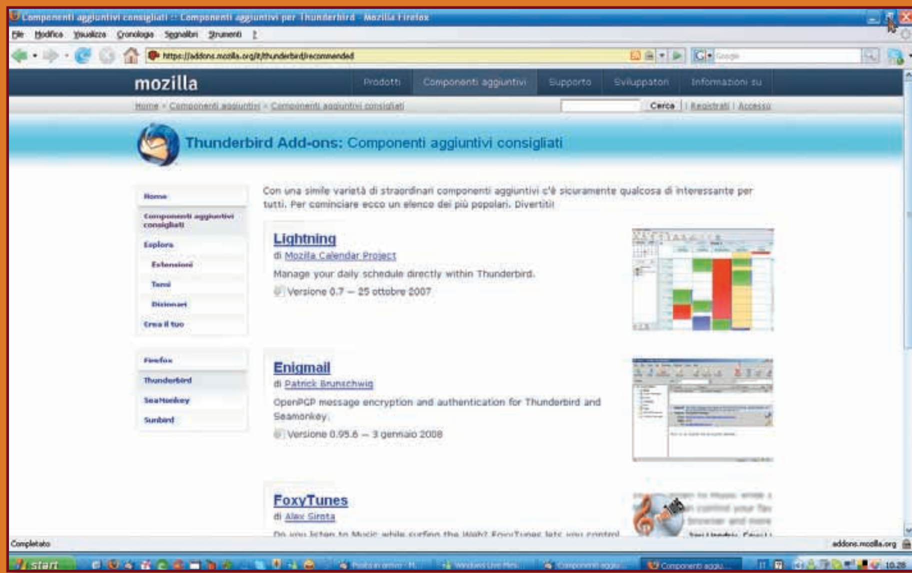
:: Radici profonde

La necessità di proteggere messaggi importanti da occhi indiscreti ha origini antiche. Già nella Bibbia si parla di un codice segreto per scrivere il nome di Babele, il codice Atbash, che si basava sull'inversione dell'alfabeto. Mentre Giulio Cesare, ad esempio, per comunicare con i suoi generali inviava messaggi cifrati sostituendo ogni lettera con quella che la seguiva nell'alfabeto di tre posizioni. Un espediente che nel corso dei secoli è stato sempre più perfezionato, fino ad arrivare alle più complesse tecniche digitali dei giorni nostri.
Il sistema di codifica adottato da Giulio Cesare è uno dei primi esempi di crittografia simmetrica. In pratica, la codifica e la decodifica del messaggio avvengono attraverso la medesima chiave. Sebbene nel corso degli anni questo sistema di codifica sia stato reso sempre più complesso tramite strumenti meccanici prima ed elettronici poi, ha un punto debole: chi intercetta la chiave di codifica può facilmente tradurre e leggere il messaggio.

:: La soluzione

L'avvento dei computer e la formidabile potenza di calcolo che offrono, hanno permesso di fare grandi

passi avanti e realizzare nuovi strumenti di protezione, tra cui un più efficace metodo nato per ovviare agli inconvenienti della codifica simmetrica. Nel 1976 due specialisti statunitensi, Diffie ed Hellmann, proposero per la prima volta un sistema di crittografia a chiave pubblica. Partendo da questa base, tre matematici, Ron Rivest, Adi Shamir e Leonard Adleman, definirono un metodo che prese il nome di cifrario RSA, dalle iniziali dei loro cognomi, e che segnò la nascita della crittografia asimmetrica o a coppia di chiavi.
In pratica questo metodo si basa sull'utilizzo dei numeri primi per creare due chiavi distinte: una per codificare il messaggio, l'altra per decodificarlo. Quella usata per codificarlo è pubblica e disponibile a tutti, mentre quella che serve al destinatario del messaggio per decodificarlo è privata e non può essere calcolata partendo dalla chiave pubblica, in quanto le due chiavi vengono assegnate dal programma di crittografia in maniera casuale. Con la crittografia asimmetrica viene superato il problema della possibile intercettazione della chiave di decodifica: il destinatario del messaggio, infatti, la possiede già.



Per proteggere le nostre email con un sistema di crittografia possiamo usare Thunderbird, il programma di posta elettronica che mette a nostra disposizione un Componente Aggiuntivo, per la codifica dei messaggi chiamato Enigmail.



:: Inviolato

Se fino al secolo scorso la necessità di sicurezza nelle comunicazioni era evidente soprattutto in ambito militare, la diffusione di Internet ha portato il tema sicurezza in primo piano. Basti pensare ai vari servizi di Home Banking, ai siti per gli acquisti online, ma anche alla posta elettronica e ai miliardi di messaggi istantanei e telefonate che ci scambiamo tutti i giorni.
Il sistema basato sul cifrario RSA è ancora oggi alla base delle comunicazioni cifrate. Il livello di sicurezza di questo metodo, infatti, è altissimo: per decifrare un messaggio protetto sarebbe necessario individuare i fattori primi della chiave pubblica. Visto che le chiavi usate oggi sono enormi (1024 o 2048 bit), individuarne i fattori primi richiederebbe tempi lunghissimi.
La caratteristica che sta alla base della sua inviolabilità, però, è anche il suo peggior difetto: i difficili calcoli necessari per la crittografia delle informazioni rendono lente le operazioni di codifica e decodifica, soprattutto nel caso in cui abbiamo a che fare con una grande quantità di dati. Per ovviare a questo limite è stata introdotta una soluzione a due passaggi: la trasmissione viene effettuata con il veloce sistema di crittografia simmetrica, mentre la più sicura e affidabile tecnica di crittografia asimmetrica è usata per proteggere la trasmissione della chiave di codifica e decodifica, impedendone l'intercettazione.

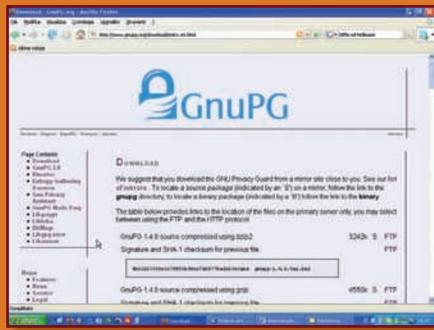
::Il più diffuso

Nel 1991, Phil Zimmerman creò quello che ancora oggi è il programma di crittografia più diffuso al mondo. Stiamo parlando di PGP, acronimo di Pretty Good Privacy. Il nome "pretty good" in inglese vuol dire "abbastanza buono" e racchiude una grande verità relativa alla crittografia: è impossibile creare un sistema sicuro in maniera assoluta, visto che le variabili che concorrono a rendere intercettabile una comunicazione sono tantissime, a cominciare dalla più frequente e imprevedibile di tutte: la distrazione umana.
PGP si basa sull'utilizzo di un doppio sistema di protezione a crittografia simmetrica e asimmetrica. Sebbene possa essere usato per rendere illeggibile il contenuto di un intero disco fisso, deve la sua fama all'efficacia dimostrata nell'ambito della protezione delle email. Di fatto, il programma nacque proprio per proteggere le comunicazioni tra Zimmerman e gli altri membri del gruppo di attivisti antinucleare al quale lo scienziato apparteneva. Per un certo periodo di tempo, l'utilizzo e la diffusione del programma furono addirittura bloccati dal Governo degli Stati Uniti: secondo il regolamento per le esportazioni di prodotti e servizi USA , infatti, un sistema di crittografia che utilizza una chiave maggiore di 40 bit è considerato un'arma, alla stregua delle munizioni.
Col tempo le cose sono cambiate: sebbene il regolamento di esportazione è immutato e ancora in vigore, i sistemi di crittografia sono ora competenza del Dipartimento del Commercio e la soglia ammessa per quanto riguarda la lunghezza della chiave è stata portata oltre i 40 bit. Il risultato di questi cambiamenti è che PGP ora non è più considerato un'arma non esportabile, ma è semplicemente soggetto alle leggi locali del paese in cui viene esportato.

:: Email protette

Lo sviluppo di PGP ha portato alla realizzazione di numerosi software per la crittografia delle email. Il più famoso e diffuso oggi è GNU Privacy Guard, una versione open source del celebre sistema di crittografia, sviluppato dalla Free Software Foundation. Il software è piuttosto spartano e usa ancora i controlli tramite righe di comando. L'ostacolo, però, può essere aggirato facilmente utilizzando uno dei numerosi plug-in disponibili per i vari programmi di posta elettronica. Il più conosciuto e affidabile è Enigmail, ideato per funzionare con Mozilla Thunderbird 2.0.

Per scaricare e installare Enigmail dobbiamo selezionare la voce Componenti aggiuntivi dal menu Strumenti di Thunderbird. Dalla finestra che compare, premiamo il link Scarica estensioni e verremo indirizzati sulla sezione download di Mozilla. Una volta scaricato il plug-in, premiamo il pulsante Installa e selezioniamo l'estensione per aggiungere la funzione al programma di posta elettronica.



Quando proteggiamo un'email usiamo gli strumenti di Enigmail, ma il vero lavoro di crittografia viene fatto dal programma GnuPG.

Per cifrare i messaggi, GnuPG utilizza una coppia di chiavi, pubblica e privata, come prevede la crittografia asimmetrica, ma sfrutta l'uso di algoritmi simmetrici che offrono una maggiore velocità nella codifica. In pratica, quando si deve proteggere un messaggio, il programma genera una chiave di sessione, per l'algoritmo simmetrico, che viene cifrata con la chiave pubblica del destinatario.

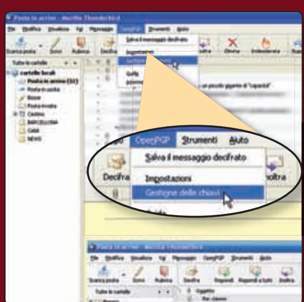
Sfruttando entrambi i metodi di crittografia, GnuPG in particolare e lo standard OpenPG in generale, consentono di ottenere un rapporto eccellente tra velocità e livello di protezione.

:: Orecchie dappertutto

Proteggere le nostre mail è il primo passo per mettere le nostre comunicazioni al riparo da eventuali curiosi, ma non è abbastanza. Se un malintenzionato può intercetare con facilità un'email, può fare la stessa cosa anche con le conversazioni telefoniche su cellulare. Nonostante gli sforzi degli sviluppatori, infatti,le caratteristiche del protocollo GSM offrono poche garanzie di sicurezza. Lo dimostrano fatti di cronaca più o meno recenti che hanno testimoniato quanto sia facile ascoltare le comunicazioni su rete GSM.

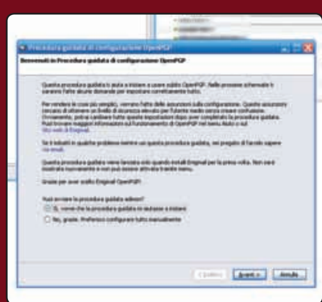
Il metodo usato per proteggere da orecchie indiscrete le telefonate si basa sugli stessi principi usati per le email: la crittografia. Quello che cambia è il modo in cui una telefonata può essere intercettata.

I PRIMI PASSI CON ENIGMAIL



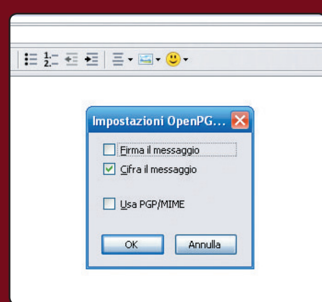
1 UN NUOVO MENU

Al termine dell'installazione di Enigmail, dobbiamo riavviare Thunderbird. Nel sistema di controlo notiamo un nuovo menu nella barra degli strumenti: OpenPGP. Cominciamo da qui selezioniando la voce Gestione delle chiavi.



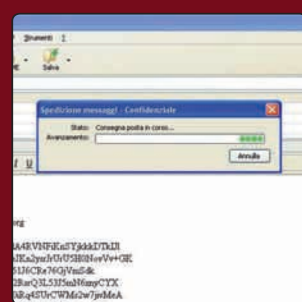
2 PROCEDURA GUIDATA

La prima volta che usiamo Enigmail, per configurare OpenPGP possiamo scegliere se avviare la procedura guidata o se fare tutto da soli. Selezioniamo la prima opzione, premiamo il pulsante Avanti e seguiamo le istruzioni.



3 SERVE UNA COPPIA DI CHIAVI

La procedura guidata prevede anche la creazione della prima coppia di chiavi necessaria per crittografare le email. Il programma richiede l'impostazione di una Passphrase che ci serve per proteggere le chiavi stesse.



4 MISSIONE COMPIUTA

La procedura può richiedere parecchi minuti. Possiamo velocizzarla navigando sul Web o usando programmi che richiedono un grande impegno al disco fisso. Tutto questo fornisce al programma dati utili per generare le chiavi.

:: Un buco nel sistema

Fino a qualche anno fa, per riuscire a intercettare una telefonata bisognava investire cifre nell'ordine dei 250.000 euro, quanto ne costava un apparecchio in grado di violare la rete GSM. Oggi le cose sono cambiate: tutto quello che serve è un normalissimo computer e il software adatto.
A cambiare le carte in tavola ci ha pensato un gruppo di ricercatori israeliani, che nel 2003 ha scoperto una falla nel debole sistema di crittografia integrato nella rete GSM. Gli scienziati hanno notato che il sistema GSM accede innanzitutto ai dati per eliminare interferenze e solo in un secondo momento effettua la crittografia. La conseguenza è che, durante la prima fase, i dati sono accessibili a tutti. L'algoritmo usato per la crittografia GSM si chiama A5 ed è ormai giunto alla sua terza versione, ma non ha ancora superato questa vulnerabilità e non consente quindi di contare su una protezione completa.

:: Difendiamoci

I soggetti che corrono il maggior rischio di subire intercettazioni illegali sono senza dubbio personaggi famosi, potenti uomini d'affari, giornalisti e politici sono le figure più a rischio. Anche chi non appartiene a una di queste categorie, però, può trovarsi nella condizione di dover proteggere le sue comunicazioni riservate. Fino a qualche tempo fa, non esistevano programmi di criptazione per cellulare e le uniche soluzioni per proteggere le comunicazioni richiedevano l'acquisto di un particolare modello di telefono, il Cryptophone, sul quale era stato installato un potente software di crittografia. Il costo di una coppia di telefoni di questo tipo, però, si aggirava intorno ai tremila euro.
Dalla fine di gennaio è invece disponibile anche in Italia PhoneCrypt di Securstar, che abbiamo avuto la possibilità di provare in redazione. In pratica si tratta di un software di crittografia telefonica basato su un sistema a chiave asimmetrica a 4096 bit, in grado di proteggere telefonate, SMS e tutti i file contenuti all'interno dello smartphone.

LA PRIMA INTERCETTAZIONE

La prima notizia sulla possibilità di violare il sistema GSM risale al 2003 quando un gruppo di ricercatori israeliani del Technion Institute of Technology di Haifa scoprì un errore nel sistema di crittografia usato per queste comunicazioni e riuscì a sfruttarlo per intercettare una telefonata. Prima di allora, molti esperti avevano tentato senza successo di violare quella che sembrava una rete che offriva eccellenti garanzie di sicurezza.

:: Come funziona

Compatibile con tutti gli smartphone basati su Microsoft Windows 5, PhoneCrypt è molto facile da usare, non richiede particolari impostazioni e richiede solo 4 MB di memoria disponibile. Affinché la telefonata sia protetta, il programma deve essere installato sia sul telefono dal quale parte la chiamata, sia su quello che la riceve. Possiamo in ogni caso tenere sempre attivo il software e impostare due diverse suonerie per differenziare le chiamate normali da quelle protette. Quando facciamo partire una chiamata sicura, infatti, il programma effettua un handshake spostando la telefonata dalla linea "normale" a quella dati. In questo periodo di tempo, i due telefoni usano un sistema di crittografia RSA a 4096 bit per scambiarsi una chiave di codifica AES a 256 bit che servirà a codificare la conversazione. Tutta l'operazione richiede solo una manciata di secondi e la chiave unica a 256 bit viene cancellata al termine della conversazione.
Il fatto di comunicare su una linea dati rappresenta un'ulteriore protezione, in quando solitamente il canale che viene controllato per intercettare le telefonate è solo quello vocale. Un'ulteriore vantaggio è rappresentato dal fatto di poter proteggere con la crittografia tutti i file contenuti nello smartphone. Una caratteristica utile in caso di smarrimento o di furto del telefono.

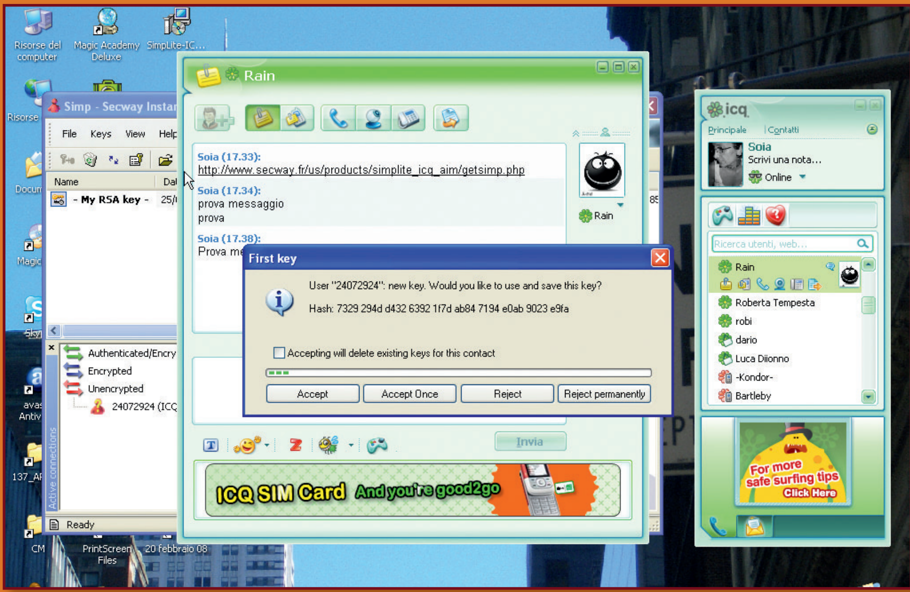
:: La qualità si paga

Uno dei principali problemi che di solito affligge i programmi di questo tipo, è la perdita di qualità dell'audio e l'eccessivo ritardo nella trasmissione della voce. PhoneCrypt offre un eccellente



Abbiamo provato a effettuare una chiamata con un telefono sul quale abbiamo installato PhoneCrypt. Il programma è compatibile con smartphone basati su Windows Mobile.

livello di protezione senza influire eccessivamente sulla qualità della voce. Dalle telefonate di prova effettuate, abbiamo potuto verificare che il ritardo nella trasmissione della voce non è tale da impedire una conversazione fluida e anche il brusio di sottofondo non risulta eccessivamente fastidioso. Ogni licenza del programma costa circa 720 euro, mentre il pacchetto che comprende sia il programma, sia il telefono, costa circa 960 euro. Se consideriamo che il prezzo degli smartphone di fascia alta si aggira intorno ai 600 700 euro, la seconda soluzione non è poi così sconveniente, soprattutto se salviamo nel telefono documenti importanti per il nostro lavoro.



Simp Lite protegge le comunicazioni automaticamente. Basta che il programma sia installato e attivo sui computer delle persone che desiderano effettuare la chat protetta.

:: Messaggi istantanei

I programmi di messaggistica istantanea come ICQ o MSN sono uno strumento pratico e versatile per comunicare con amici, colleghi o clienti, in maniera più rapida ed efficace rispetto alla classica email.

Tutti i messaggi che mandiamo con questo genere di programmi, però, viaggiano su Internet "in chiaro" e possono essere facilmente intercettati. Anche in questo caso, però, possiamo ricorrere alla crittografia.



Dal sito www.secway.fr/us possiamo scaricare Simp Lite, un programma gratuito che ci permette di proteggere le nostre chat, disponibile in diverse versioni compatibili con i programmi di Instant messaging più diffusi.

Esistono numerosi software in grado di fornire questa funzione, ma all'indirizzo www.secway.fr/us possiamo scaricare e installare Simp Lite, un o dei programmi più efficaci in grado di crittografare le dei più comuni programmi, come ICQ, MSN o Yahoo! Messenger.



Attenzione però: quando scarichiamo Simp Lite, assicuriamoci di scegliere la versione corretta per il programma di chat che usiamo. Il programma è in inglese, ma l'installazione e la configurazione sono gestite da un'efficace procedura guidata. Durante le impostazioni ci viene chiesto di inserire una parola chiave per proteggere le chiavi generate casualmente dal programma. Per inviare e ricevere messaggi criptati con Simp Lite, è necessario che anche i nostri contatti abbiano installato il programma sul proprio computer. Al termine della procedura di installazione siamo subito pronti per effettuare "conversazioni sicure" con amici o colleghi usando il programma Istant messenger come siamo abituati a fare. ■

SPEEDCABLING

Dopo il lancio dell'hard disk ecco un'altra disciplina atletica da veri geek

"Lo Speedcabling è uno sport agonistico in cui i partecipanti gareggiano nel districare una matassa di cavi." È questa la descrizione ufficiale di una pazza e tecnologica neodisciplina sportiva creata da Steven Schkolne.

L'idea risale ad un paio d'anni fa quando Schkolne, che lavora come amministratore e consulente per l'IT nella zona di Los Angeles, ha pensato che forse non era l'unico a considerare una sfida ed un piacere il combattere con grovigli di cavi di alimentazione sul retro dei PC o che penzolano da armadi stipati di router e switch.

Un rapido giro di domande tra i colleghi e la scoperta che c'era effettivamente interesse a organizzare gare di abilità e velocità per scoprire chi era il "re dei cavi": è nato così lo Speedcabling (http://www.speedcabling.org/) con le sue regole e dopo un po' anche le prime gare ufficiali.



:: Le regole del gioco

Gli "atleti" devono confrontarsi con un gomitolo di sei cavi di rete di lunghezze varie. L'obiettivo è quello di separarli il più in fretta possibile e di alzare sopra la testa e mostrare a tutti il cavo libero da nodi. La mossa serve oltre che al giudice anche a dare un segnale di vittoria. Ovviamente alla fine i cavi devono anche essere integri e vanno poi provati per accertarsi che non siano stati danneggiati nella foga della competizione.

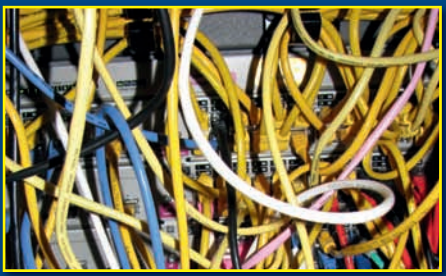
:: Cavi regolamentari

Lo speedcabling prevede due tipi di gare.
In quelle base ci si deve cimentare con una combinazione di sei cavi di rete, costituiti da due coppie da due metri, due da quattro metri e due da sette e mezzo. Il livello superiore prevede invece le stesse lunghezze ma il doppio di cavi, ben dodici, in gruppi di quattro
I cavi ethernet devono essere CAT-5 e gli atleti possono usare i propri cavi purché capaci di condurre segnali da 100Mb/s, prima e dopo la gara.

:: Preparare la sfida

Per "preparare" la sfida e riproporre le situazioni in cui spesso ci si trova nella vita reale (cavi U, seriali, di rete) in uffici, postazioni scolastiche, laboratori, centri di calcolo, sale server, lo Speedcabling ha regole ferree di "bundling", di aggrovigliamento, all'insegna dell'uniformità e della metodologia.

◄ Ecco una bella sfida - Foto di Ken Stein (www.flickr.com/photos/kenstein/)



▲ Groviglio nel datacenter - Foto di BRPhoto

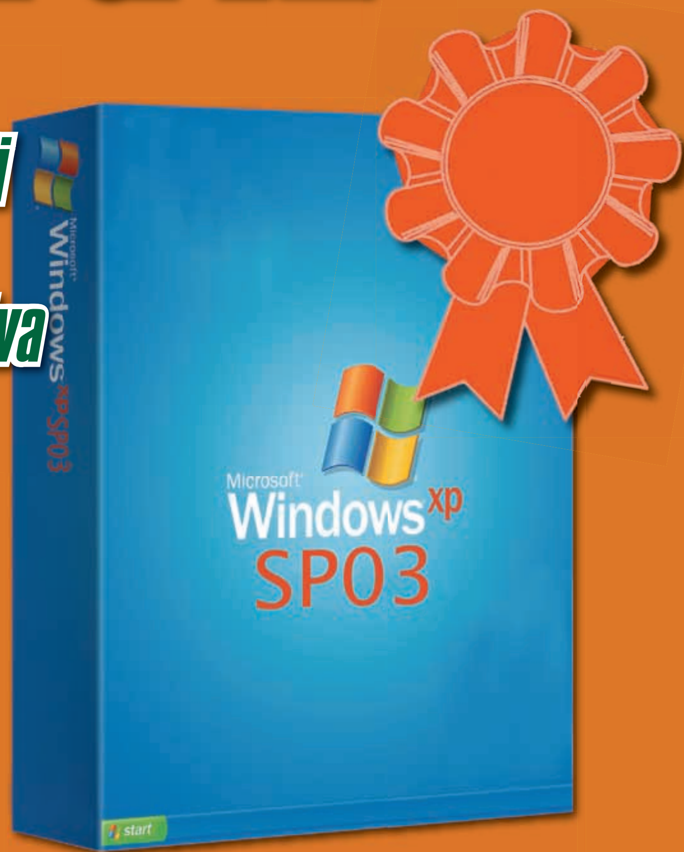
:: I passi sono due.

Anzitutto si distendono i cavi che vengono presi per una delle estremità e poi avvolti in giri lunghi all'incirca un metro. Segue l'aggrovigliamento che si effettua presso una lavanderia pubblica. I cavi regolarmente avvolti vengono infilati in una asciugatrice. Qui vengono fatti girare al massimo per circa tre minuti con il risultato di una matassa davvero intricata e ben compatta. L'ultima fase è quella di far raffreddare i cavi e infine di porre su un tavolo le matasse, davanti agli atleti che non aspettano che il fischio dell'arbitro per far partire la sfida. ■

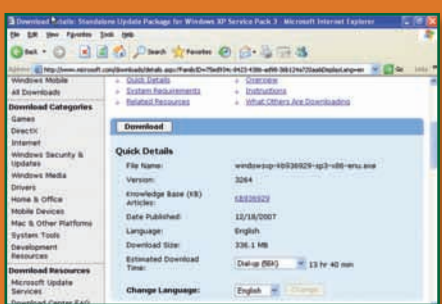


Lunga vita a XP

Con l'arrivo di Vista lo davano tutti per spacciato. Ma gli utenti Windows sembrano aver scelto il male minore ed ecco che arriva per loro il Service Pack 3



Neanche l'arrivo di Vista è riuscito a logorarlo: a sette anni dal suo debutto, Windows XP è considerato il sistema operativo Microsoft più affidabile e versatile. Dopo qualche mese in cui circolavano voci su un "abbandono" dello sviluppo, è invece arrivata la notizia del rilascio di un terzo Service Pack dedicato al caro vecchio XP, che dovrebbe dargli una marcia in più in termini di prestazioni.



Se decidiamo di scaricare la versione beta, prepariamoci a un download impegnativo: si tratta infatti della versione "completa" che integra gli aggiornamenti introdotti anche con SP1 e SP2.

:: C'è ma non si vede

Con i precedenti Service Pack, Microsoft ci aveva abituato a una serie di cambiamenti, spesso radicali, come il sistema di gestione delle reti senza fili introdotto con il Service Pack 2. Il terzo aggiornamento del sistema operativo, invece, punta a migliorare le prestazioni, le funzioni e la sicurezza senza modificare in alcun modo l'ambiente di lavoro. La maggior parte delle modifiche avverrà quindi "sotto il cofano" del nostro sistema operativo senza che apparentemente cambi nulla. In questo modo Microsoft può garantire aggiornamenti più leggeri sia in termini di spazio sia di tempo richiesti per la configurazione, una filosofia analoga a quella del recente Service Pack 1 di Windows Vista, presto disponibile anche in italiano.

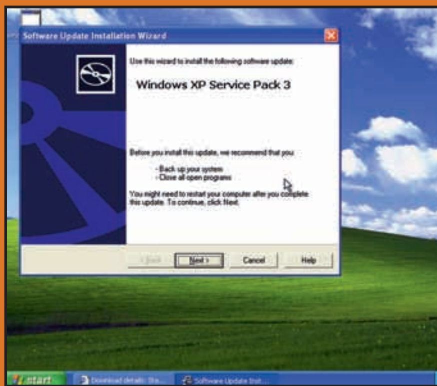
:: Non definitivo

Nel momento in cui scriviamo, il Service Pack 3 non è ancora disponibile nella versione definitiva, prevista solo per il prossimo giugno. Dal sito Microsoft, però, è possibile scaricare la versione RC2, una "beta" che è stata messa a disposizione di tutti a partire da febbraio. Comunque, il rilascio di una versione beta è un passo che gli sviluppatori Microsoft compiono solo quando sono vicini al prodotto finito. La funzione di questa distribuzione online, infatti, è ottenere indicazioni da parte degli utilizzatori per rimuovere eventuali difetti e "limare" il programma.
Se vogliamo installarla, la possiamo scaricare dal sito ufficiale di Microsoft, www.microsoft.com effettuando una ricerca con la chiave Windows XP Service Pack 3 Release Candidate. Purtroppo, però, richiede Windows XP nella versione in lingua inglese.
Naturalmente quando uscirà la versione definitiva sarà tutto più semplice. Oltre a essere fornito attraverso gli aggiornamenti automatici sarà possibile scaricare il Service Pack in un solo pacchetto e addirittura includerlo in un CD di installazione grazie alla tecnica

dello Slipstream. L’aggiornamento può avvenire da qualunque versione di Windows XP, anche se non dispone dei Service Pack precedenti. SP3 contiene tutti gli aggiornamenti di sicurezza introdotti dal lancio di XP a oggi e una serie di nuove funzioni fondamentali.

:: Nuove caratteristiche

La maggior parte delle novità introdotte da SP3 riguarda la sicurezza del sistema, ma troviamo anche alcune nuove funzioni indispensabili per garantire la convivenza di Windows XP con i sistemi operativi più recenti. Fra queste la più interessante è l’introduzione del meccanismo chiamato Network Access Protection o più semplicemente NAP. Questo metodo di autenticazione, introdotto in Windows Server 2008 permette a una rete di computer di bloccare l’accesso dei PC collegati in base al loro “stato di salute”. Gli amministratori possono decidere, per esempio, di autorizzare solo i PC con il sistema operativo aggiornato o equipaggiati con un antivirus funzionante. Senza questo aggiornamento, i computer dotati di Windows XP sarebbero tagliati fuori dalle reti basate sui nuovi server Microsoft.



Anche nelle prime fasi dell’installazione non cambia molto rispetto ai pacchetti più vecchi. Possiamo effettuare l’aggiornamento anche se siamo privi dei Service Pack precedenti.

:: Qualità nascoste

Le altre novità introdotte dal nuovo Service Pack riguardano soprattutto aspetti tecnici del sistema operativo. La prima e più interessante riguarda le nuove installazioni. Usando i CD con SP3 integrato infatti sarà possibile installare Windows XP senza bisogno di inserire subito il codice di attivazione. Questo metodo è analogo a quello di Vista, che permette di registrare il prodotto fino a trenta giorni dopo l’installazione. Il kernel, cuore del sistema operativo, cambia includendo alcuni algoritmi crittografici, anche se le implicazioni di questa modifica al momento non sono ancora state rese note. L’ultimo aggiornamento “innovativo” riguarda la possibilità di ignorare i black hole router, ovvero i dispositivi di rete che inviano alcuni tipi di pacchetti non corretti. Questa funzione dovrebbe rendere più efficiente e affidabile la gestione delle reti, contribuendo anche a combattere gli attacchi Denial of Services, usati spesso dai pirati informatici per “abbattere” i server Web.

:: Qualcosa cambia

Oltre alla compatibilità con nuovi sistemi di sicurezza, SP3 introduce alcuni accorgimenti che permettono una migliore gestione delle risorse, che comporta un certo incremento nelle prestazioni del PC. Un bel cambiamento rispetto al vecchio Service Pack 2, che secondo molti utilizzatori avrebbe rallentato il sistema. Purtroppo questo miglioramento è difficile da quantificare e varia anche in funzione dei programmi installati e della configurazione del computer sul quale viene installato. Utilizzando una macchina con Service Pack 3, però, si ha l’impressione di un effettivo aumento dell’efficienza, quasi come se ci si trovasse di fronte a un sistema appena installato. ■

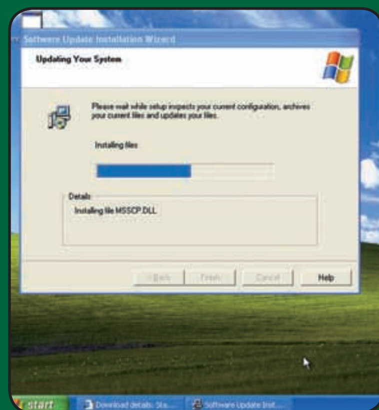
AGGIORNAMENTI FACOLTATIVI

Oltre agli aggiornamenti del sistema operativo, il Service Pack 3 ne introduce anche alcuni per altri software Microsoft. L’aggiornamento, naturalmente, è facoltativo: questo significa che se abbiamo già installato Internet Explorer 7 o Windows Media Player 11 saranno aggiornati, ma non siamo costretti ad averli per installare il Service Pack. Grazie alle nuove caratteristiche, possiamo sicuramente aspettare qualche tempo prima di mandare in pensione il PC con Windows XP.



NESSUN CONTROLLO?

Una cosa che ci colpisce quando scarichiamo e installiamo la RC2 del Service Pack 3 è la mancanza del controllo Microsoft genuine, il modulo che verifica l’autenticità del sistema operativo. Non si tratta di un cambio nelle politiche di Microsoft, ma di un’usanza ormai consolidata. Il controllo viene effettuato solo quando scarichiamo aggiornamenti ufficiali e non nel caso di versioni beta.



Hack++

C++, caratteristiche a oggetti

Ciò che è alla radice del C++ è la programmazione a oggetti, che lo differenzia dal C

Il C++ fu inventato da Bjarne Stroustrup nei laboratori Bell di Murray Hill. Egli non aveva la presunzione di creare un nuovo linguaggio di programmazione, ma bensì di potenziarne uno già esistente e di grande successo: il C. Stroustrup aggiunse alle caratteristiche più vantaggiose del C tutta la potenza della programmazione a oggetti, quindi si può dire che il C++ è la versione a oggetti del C. Questo ha reso molto agevole l'apprendimento del C++ da parte dei programmatori C, i quali dovettero solo comprendere il concetto di programmazione a oggetti.

In poche parole, comunque, la programmazione a oggetti attinse ai concetti migliori della programmazione strutturata e introdusse altri concetti del tutto nuovi, cambiando completamente, e positivamente, il modo di organizzare un programma.

Parlando più in generale, esistono due modi di organizzare un programma: attorno al codice o attorno ai dati in proprio possesso. La programmazione strutturata consente generalmente di organizzare il programma attorno al codice. La programmazione a oggetti ha introdotto il concetto opposto, cioè sono i dati che controllano il programma. Vediamo meglio come: tutti i linguaggi di programmazione orientati agli oggetti hanno tre caratteristiche comuni: incapsulamento, polimorfismo ed ereditarietà. Esaminiamole una per una.

:: Incapsulamento

L'incapsulamento è un meccanismo che consente di racchiudere dati e routine in un blocco protetto da interferenze esterne, quindi dalle manipolazioni da parte di codice che non fa parte di questo "blocco". Il blocco prende il nome di classe, quindi possiamo dire che il codice e i dati collegati tra loro all'interno di una classe costituiscono un oggetto, o più semplicemente, un oggetto è un'istanza di una classe.

All'interno di una classe i dati e il codice possono essere privati o pubblici. I dati privati sono noti solo all'interno della classe stessa, mentre se sono pubblici possono essere manipolati anche da codice che non fa parte della classe. Essenzialmente i dati pubblici sono un'interfaccia per interagire con le parti private dell'oggetto. La forma di una classe in C++ è questa:

```
class nomeclasse{
                                dati e funzioni private
                                public:
                                dati e funzioni pubblici
                                } lista oggetti;
```

Il codice e i dati che fanno parte di una classe sono detti membri della classe. Le variabili sono chiamate specificamente variabili d'istanza, rappresentano i dati contenuti da una classe.

:: Polimorfismo

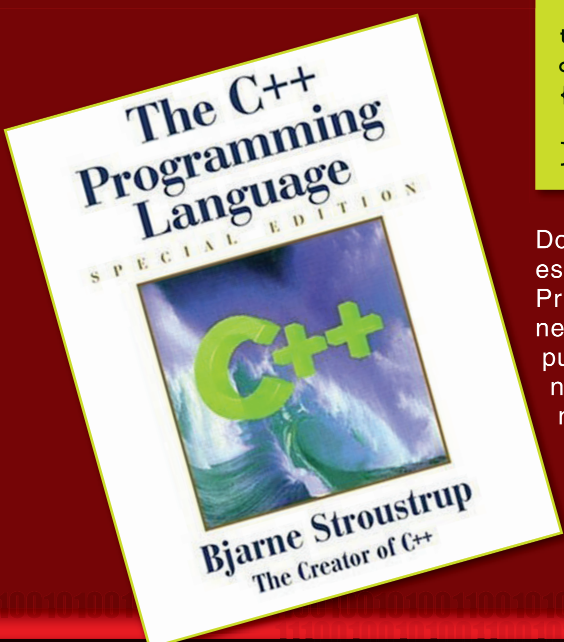
Dal greco, "pluralità di forme", è la funzionalità che consente al programmatore di accedere ad un'intera classe di azioni. Faccio un esempio banale che ho letto su un manuale di programmazione: prendiamo il volante di un'automobile (l'interfaccia), è lo stesso qualsiasi sia il meccanismo di sterzo effettivamente utilizzato. Vale a dire che il volante funziona sempre allo stesso modo, sia che abbiate uno sterzo manuale o il servosterzo. Ciò fa si che imparando ad utilizzare un volante, l'automobilista sarà in grado di guidare qualsiasi tipo di automobile. Ecco, il polimorfismo permette di avere un'interfaccia uniforme, come il volante di un'automobile, anche in programmazione.
Il concetto di polimorfismo viene sintetizzato nella famosa espressione "un'interfaccia, molti metodi". Vale a dire che si può creare un'interfaccia comune per diverse attività tra loro collegate.
Quindi lo sforzo sta solo nel ricordare l'interfaccia generale, delegando il compilatore la scelta dell'azione specifica da applicare in ogni situazione.
In C++ il polimorfismo è consentito dall'utilizzo della tecnica di overload. Questa tecnica è applicata generalmente alle funzioni e agli operatori. Per quanto riguarda le funzioni, consente di dare a due o più funzioni lo stesso nome, a patto che abbiano diverse dichiarazioni di parametri. Si può dire quindi che si dichiarano diverse versioni della stessa funzione. Per chiarire le idee propongo un esempio:

```
...
void funz(int a);
void funz(int a, int b);
void funz(char t)
...
```

La funzione funz è soggetta a overload tre volte, fate caso alle liste di parametri diverse tra loro.
Ovviamente ognuna esegue un compito indipendente dalle altre. Generalmente si consiglia di sottoporre a overload solo funzioni che eseguono funzioni strettamente colelgate, o magari la stessa funzione su diversi tipi di dato. Eseguire l'overload su due funzioni che non c'entrano niente l'una con l'altra è considerata mancanza di stile.
L'overload di operatori è strettamente collegato all'overload di funzioni. Per sottoporre a overload un operatore è necessario definire il significato dell'operazione che effettua all'interno di una classe dichiarata. La forma generale è la seguente:

```
tipo nomeclasse:: ☠
operator#(lista-argomenti)
{
  //operazioni
}
```

Dove a # va sostituito l'operatore ad esempio +, – o !=.
Prima di passare all'ereditarietà, è necessario parlare di un errore che può verificarsi facendo uso delle tecniche di overload. Si tratta di problemi di ambiguità, cioè che il compilatore potrebbe non trovarsi in grado di effettuare una scelta della funzione giusta da usare. Questo errore dal punto di vista tecnico non può essere evitato in nessun modo, solo l'esperienza insegna a giudicare bene come dichiarare una lista di parametri.



:: Ereditarietà

"L'ereditarietà è il processo mediante il quale un oggetto acquisisce le proprietà di un altro oggetto in base al concetto di classificazione gerarchica".
Questa è la definizione di ereditarietà, ma se ci pensiamo un attimo è immediato capire come ogni cosa fa parte di una classificazione gerarchica. Prendiamo ad esempio una vipera, fa parte della classe serpenti, che a sua volta fa parte della classe rettili, che fa a sua volta parte della grande classe animali. Ogni sottoclasse della classe animali assorbe la proprietà della classe gerarchicamente superiore, aggiungendone delle altre, fino ad arrivare all'elemento singolo che ha gli elementi che lo rendono unico più tutti quelli acquisiti dalle classi superiori.

In programmazione se non ci fosse la classificazione gerarchica, in ogni oggetto dovrebbe essere dichiarata ogni sua caratteristica. Invece grazie all'ereditarietà è necessario solo specificare quelle caratteristiche che lo rendono unico all'interno della sua classe. Pertanto un oggetto può rappresentare un esempio specifico di una classe più grande.

I modi descritti in questo articolo in cui il C++ sfrutta le caratteristiche ad oggetti sono solo una parte che copre la maggioranza dei casi, ma bisogna tenere a mente che non è l'unica strada che è possibile seguire. Per esempio l'incapsulamento può essere praticato anche attraverso strutture o union. ■

☠ Attenzione!!!
Esigenze grafiche ci hanno costretti a spezzare questa riga di codice.

SPAZZATURA ITALIANA

Italia, patria di santi, poeti, navigatori e... spammatori incalliti!

Se pensavamo che il problema della spazzatura riguardasse solo Napoli e dintorni, ci siamo sbagliati. Basta dare un'occhiata alla nostra casella di posta elettronica per cambiare idea! Purtroppo, l'impressione di essere bersagliati da email indesiderate (e pericolose) è confermata da una ricerca scientifica condotta a livello globale. Sophos, azienda specializzata nel settore della sicurezza informatica, ha pubblicato il nuovo rapporto sullo spam mondiale e, tra i dodici paesi più infestati da questa spazzatura, ci siamo anche noi! Ma la cosa che più preoccupa del rapporto sull'ultimo trimestre del 2007 è che l'Italia ha guadagnato addirittura sei posizioni rispetto al periodo precedente, in cui era solo tredicesima. Tradotto in numeri, abbiamo prodotto il 3,5% dello spam mondiale e siamo a ridosso della Turchia, che ci precede con il 3,8%. Naturalmente non possiamo sperare di eguagliare il record degli Stati Uniti, che sono primi assoluti con il 21,3%, ben lontani dalla Russia (seconda con l'8,3%), ma ci stiamo davvero impegnando. A cosa è da attribuirsi questa crescita esponenziale? Secondo Walter Narisoni, dirigente di Sophos Italia, la causa è una mancanza di difese nei nostri computer. Ancora troppe persone affrontano i pericoli di Internet pensando che basti non frequentare certi siti per stare tranquilli. Oppure sono del tutto allo scuro del problema. Invece la realtà è ben diversa perché dall'altra parte della barricata ci sono criminali che con queste attività illecite ci guadagnano moltissimo e che possono contare su intere reti di computer per lanciare le loro campagne di spam.

In pratica, dovremmo trattare Internet come se fosse un'arma carica e pronta a sparare, così eviteremo di farci male e di favorire la diffusione dello spam. Si tratta solo di prendere le opportune precauzioni, come non aprire e-mail di cui non conosciamo il mittente. Ma è anche necessario installare nel nostro computer tutti quei sistemi di difesa che ci possono proteggere efficacemente dalla spazzatura informatica e tenerli rigorosamente aggiornati. Sì, di solito sono a pagamento, ma sono i soldi meglio spesi per la sicurezza del PC. ■



Le TRAPPOLE del commercio online
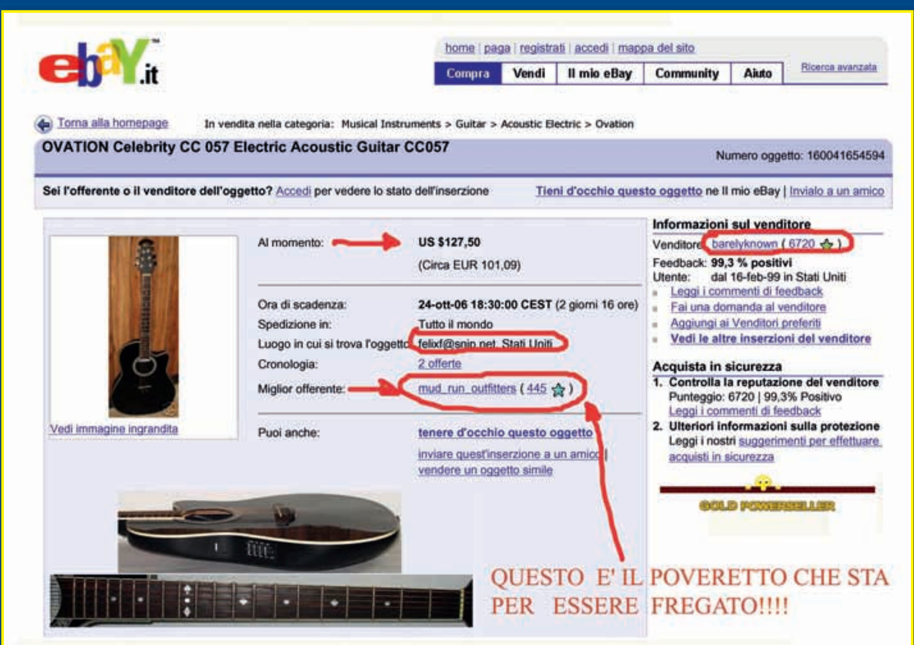
Dalla Spagna un nuovo allarme per chi compra su Internet



Il fenomeno del commercio on-line sta crescendo in maniera esponenziale e sempre più utenti lo praticano, non sempre in maniera responsabile. La molla che spinge a comprare in Internet è spesso la convenienza dei prezzi (vera o presunta), ma dietro certi affari incredibili può nascondersi la truffa. Quella più classica è promettere un bene, farselo pagare e poi non consegnarlo, Striscia la Notizia proprio qualche settimana fa ha sbugiardato un "simpatico personaggio" che agiva in questo modo indisturbato da ormai parecchio tempo. Ma da questo raggiro è facile difendersi, perché esistono sistemi di pagamento (per esempio PayPal) che proteggono sia il venditore, sia il compratore.

Esistono però altri metodi più sofisticati, che colpiscono soprattutto gli utenti meno smaliziati. Uno dei più diffusi è il phishing, cioè quel tipo di truffa che ci invita a comunicare i nostri dati sensibili (come le coordinate bancarie) a siti fasulli, ma molto simili a quelli, per esempio, di istituti di credito. Uno degli ultimi casi di truffa informatica è avvenuto in Spagna e ha portato all'arresto di 76 persone, appartenenti a una quindicina di organizzazioni criminali diverse. L'azione della polizia postale spagnola è stata fulminea ed efficace, impedendo così ai delinquenti di fare perdere le loro tracce. Tra l'altro, questa operazione, chiamata Ulises, ha stabilito un vero record in fatto di malviventi arrestati in un colpo solo. Purtroppo, la ragione di una simile "pesca miracolosa" è dovuta al fatto che la Spagna è uno dei paesi al mondo dove ci sono più frodi bancarie su Internet. Un altro record poco invidiabile del paese iberico è la grande diffusione di Botnet, cioè quelle reti controllate a distanza da cybercriminali in cui spam e phishing sono all'ordine del giorno.

Di fronte a questi fenomeni sempre più diffusi, è chiaro che dobbiamo prendere le dovute precauzioni. Gran parte del commercio online è onesto e sicuro, quindi possiamo continuare a fare tranquillamente i nostri acquisti. Tuttavia è sempre più necessario avere un computer protetto da sistemi di difesa efficaci (antivirus, firewall, antispyware...) e non fornire mai i nostri dati personali. Insomma, aiutiamoci, che la tecnologia ci aiuta. ■



Emuliamo WORLD OF WARCRAFT su UBUNTU

Questo articolo illustra come emulare su Ubuntu 7.04 Feisty Fawn il client di World of Warcraft, essenzialmente gli stessi princìpi dovrebbero valere anche per le altre distribuzioni



La prima cosa necessaria è l'emulatore della piattaforma Microsoft, possiamo far uso di Wine, emulatore open source e completamente gratutito. Sotto Ubuntu lo installiamo tramite:

```
sudo apt-get install wine
```

In caso la vostra lista repo sia obsoleta, potete sempre aggiornarla tramite:

```
sudo apt-get update
```

Dopo aver installato il software necessitate di configurare l'audio in modo che sfrutti le librerie del sistema operativo, quindi:

```
winecfg
```

Andate alla scheda audio e spuntate la casella OSS.
Procuratevi le seguenti due DLLs e mettele in /home/utente/.wine/drive_c/windows/system32:

```
msvcp60.dll;
mfc42.dll;
```

Ora è arrivato il momento di installare il gioco. Dopo esservelo procurato, lo installerete emulando il programma di installazione, quindi:

```
wine installer.exe
```

Installatelo sotto /home/utente/.wine/drive_c. Una volta installato editare il file World of Warcraft/WTF/Config.wtf, aggiungendo le seguenti informazioni:

```
SET gxApi "opengl"
SET SoundOutputSystem "1"
SET SoundBufferSize "100"
```

Se volete perfezionare il tutto, seguite questo procedimento: 1. Aprite wine regedit; 2. Cercate HKEY_CURRENT_USER/Software/Wine; 3. Aggiungete la chiave "OpenGL"; 4. Aggiungete il valore stringa "DisabledExtensions" e dategli il valore "GL_ARB_vertex_buffer_object";



Ora potete creare un'icona d'avvio, assegnandole il seguente comando:

```
wine /home/utente/.wine/
drive _ c/worldofwarcraft/
wow.exe -opengl
```

Lord Hk

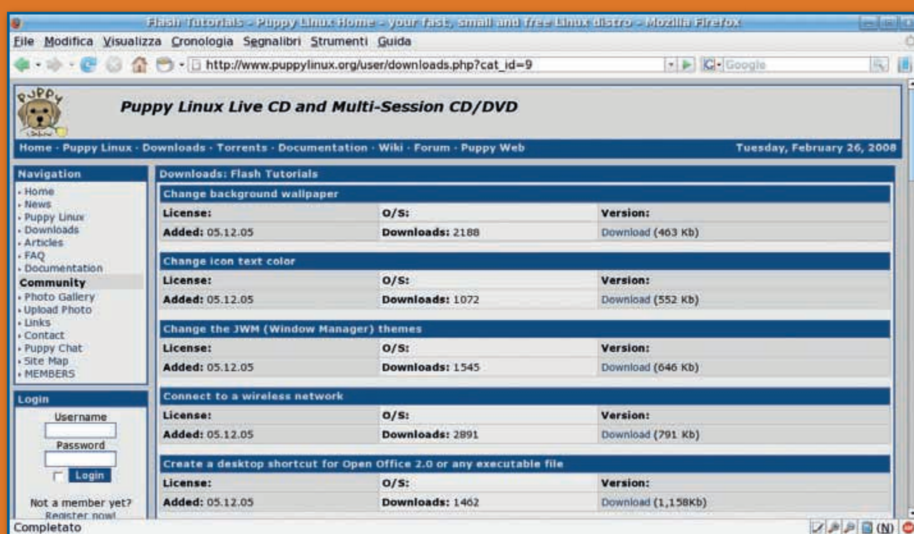
Attenzione!!!
Esigenze grafiche ci hanno costretti a spezzare questa riga di codice.

Mettiamo Puppy nella penna



Scopriamo le virtù di Puppy, un completo sistema operativo in meno di 100Mega di spazio!

I possibili utilizzi di un sistema operativo in miniatura sono molteplici: si va dal recupero di documenti inaccessibili (a causa, ad esempio, dell'impossibilità di riavviare correttamente il sistema operativo su hard disk) all'installazione su di una chiavetta USB per avere un sistema completo sempre disponibile, fino al puro e semplice piacere di sperimentare nuovi software e nuove tecnologie. In questo articolo, quindi, faremo la conoscenza di Puppy Linux, una mini-distribuzione Linux davvero interessante: possiamo installarla su di una penna USB anche di ridotta capienza (bastano 128MB disponibili!) ed il sistema ridurrà al minimo le operazioni di scrittura sul dispositivo, così da aumentare la durata di questo; come si sa, infatti, le memorie flash nelle chiavette hanno un numero non altissimo di cicli di scrittura possibili. Altra caratteristica di spicco di Puppy Linux è il caricamento in ram dell'intero sistema: ciò consente di liberare il lettore CD/DVD e di poter inserire, così, altri supporti.



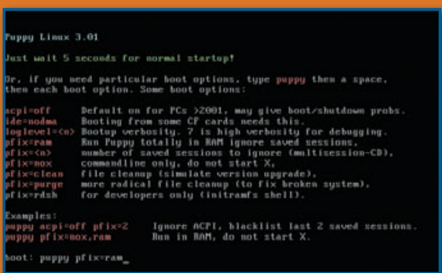
Il sito di Puppy Linux è davvero ricco di informazioni: ci sono addirittura dei tutorial in flash!

:: Installiamo Puppy!

Puntiamo con il nostro web browser preferito sul sito di Puppy Linux, http://www.puppylinux.org, ed entriamo nella sezione "Downloads".

Nella nuova schermata clickiamo su "Puppy Linux Main Release" e scarichiamo l'ultima release del sistema operativo disponibile, attualmente la 3.01; andremo a prelevare un'immagine ISO, un file cioè che rappresenta l'intera immagine di un supporto CD.

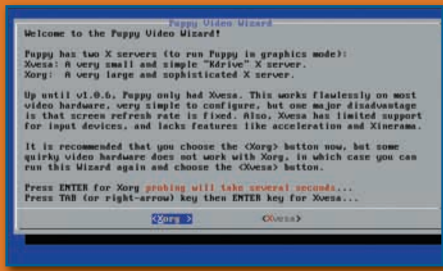
La release 3.01 è disponibile in due versioni, puppy-3.01-seamonkey.iso e puppy-3.01retro-k2.6.18.1-seamonkey.iso: la prima è la versione standard, la seconda presenta un kernel meno aggiornato; se vediamo che la prima versione ha problemi a funzionare con il nostro hardware, proviamo con la seconda.Una volta scaricata l'immagine ISO non ci resta che masterizzarla su CD con il programma che preferiamo. Fatto questo, spegniamo il PC, inseriamo il CD nel lettore e riavviamo la macchina. Apparirà la schermata di avvio di Puppy Linux: attendiamo 5 secondi per far avviare il sistema operativo con le opzioni di default, altrimenti digitiamo 'puppy pfix=ram' per caricare l'intero SO in ram oppure 'puppy acpi=off' se scopriamo che Puppy non riesce ad avviarsi o ad effettuare la procedura di shutdown correttamente.



La schermata di boot di Puppy Linux. Nell'esempio carichiamo l'intero SO in ram.

:: Avviamo il sistema

Prima di poter accedere al desktop di Puppy è necessario fornire qualche informazione aggiuntiva al sistema. Innanzitutto, comparirà una schermata in cui dovremo selezionare il tipo di tastiera sul nostro PC: quella di default è la tastiera americana ('us'), per indicare quella italiana scegliamo dall'elenco 'it'. Ci verrà poi chiesto di selezionare la modalità video che il sistema deve utilizzare, Xorg o Xvesa; la prima ha prestazioni migliori mentre la seconda ha un maggiore grado di compatibilità con l'hardware. Proviamo con Xorg e passiamo ad Xvesa in caso di problemi nella visualizzazione dello schermo. Alla comparsa del desktop di Puppy, quindi, scegliamo la risoluzione video che più ci aggrada.



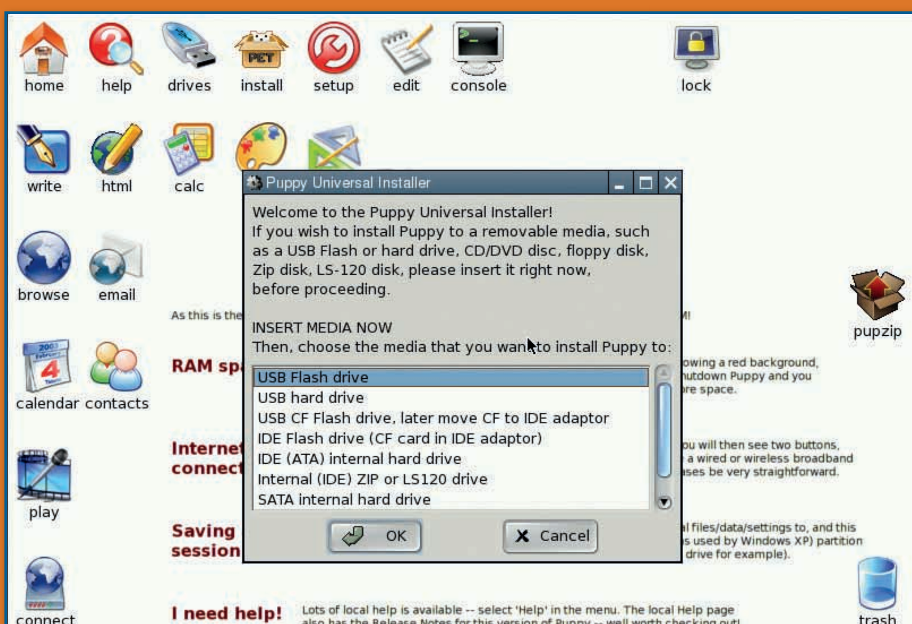
La scelta della modalità video. Proviamo con Xorg e se non funziona ripieghiamo su Xvesa.

:: Installazione sulla chiavetta

Il desktop di Puppy ha un'organizzazione degli elementi piuttosto standard: le icone per i programmi e le funzionalità principali sulla scrivania, quindi il menu principale in basso inserito nel classico pannello di sistema. Presa confidenza con l'interfaccia grafica, andiamo subito ad installare il nostro sistema operativo in miniatura su di una chiavetta USB. Inseriamo la penna nel PC, quindi clickiamo sul 'Menu' in basso ed entriamo nella sezione "Setup": qui clickiamo sulla voce "Puppy Universal Installer".
Comparirà la finestra "Puppy Universal Installer": qui clickiamo sulla voce "USB Flash drive" e premiamo "OK". Selezioniamo il dispositivo della chiavetta ("sda Usb 2.0 Flash Disk", ad esempio), quindi nella schermata successiva clickiamo sull'icona "Install Puppy to sda1:" (chiaramente, il file di dispositivo può essere diverso da sda1). Schiacciamo "OK". Ci verrà richiesto di indicare dove sono i file del sistema operativo, se nel CD o in una directory: dato che abbiamo effettuato il boot dal Live CD, clickiamo su "CD". A questo punto, se abbiamo tolto il CD di Puppy dal lettore reinseriamolo e clickiamo su "OK".

:: MBR e dintorni

L'Installer adesso ci chiederà se copiare un MBR alternativo sulla penna: il MBR (Master Boot Record) è il settore di avvio di un dispositivo ed è ciò che ci consentirà di far avviare Puppy dalla chiavetta. Nella gran parte dei casi, la scelta di default è quella giusta ma, nel caso non riuscissimo a far partire il sistema dalla penna USB, possiamo provare una dopo l'altra le altre opzioni disponibili. Fatto questo, l'Installer controllerà se sul dispositivo prescelto la prima partizione presente abbia o meno il flag 'boot' attivo: in caso negativo, dovremo attivarlo lanciando il



L'Universal Installer di Puppy. Per installare il sistema su una chiavetta USB.

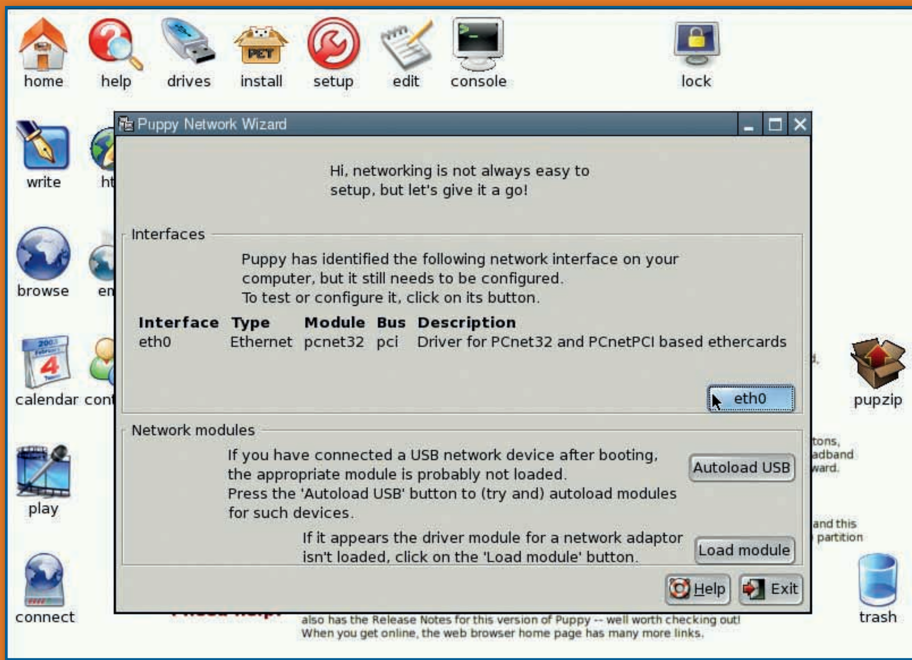
programma GParted: nella finestra di questo, molto semplicemente, clickiamo con il tasto destro del mouse sulla riga relativa alla prima partizione della penna (ad esempio, /dev/sda1) e dal menu che compare selezioniamo la voce “Manage flags”; quindi mettiamo la spunta sull’opzione “boot”.

:: Gli ultimi passaggi

Nella schermata successiva ci viene suggerito di selezionare l’opzione di default e clickare “OK” per proseguire; se vogliamo, però, possiamo prima richiamare nuovamente GParted (opzione “GParted”) per cancellare e ricreare la partizione su cui copiare Puppy Linux: questo può servire nel caso in cui il sistema operativo su penna USB non riuscisse ad avviarsi. Eccoci arrivati alla fine. Apparirà una finestra arancione che ci chiederà, finalmente, di confermare l’installazione di Puppy: schiacciamo Invio sulla tastiera ed attendiamo con la copia dei file sulla chiavetta abbia termine. Adesso possiamo riavviare il PC.

:: Attiviamo la connessione alla rete

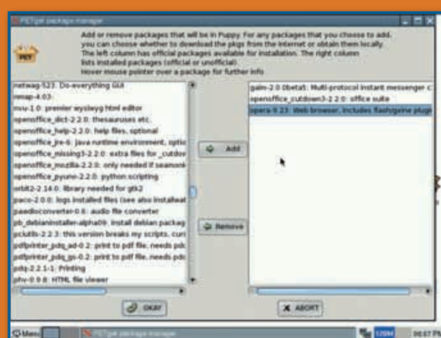
Ora che Puppy Linux è sul nostro piccolo dispositivo tascabile, scopriamo come utilizzare al meglio questo sistema operativo. Innanzitutto, clickando sull’icona “browse” sul desktop noteremo come non venga attivata alcuna connessione di rete per default: per rimediare, clickiamo sull’icona “connect” in basso sulla scrivania; comparirà una finestra in cui potremo configurare un collegamento via modem analogico o ADSL. Se utilizziamo un modem/router ADSL con server DHCP, ad esempio, clickiamo sull’icona a fianco della scritta “Connect to internet by network interface”, quindi nella schermata successiva premiamo il pulsante indicante l’interfaccia di rete connessa al modem/router (eth0, ad esempio); infine, clickiamo su “Auto DHCP”.



Attiviamo la connessione ad Internet...

:: Il software

Pur se sviluppato per ridurre al minimo le richieste di spazio sui supporti, Puppy Linux ha un parco software di tutto rispetto: Abiword come word processor (legge e scrive documenti RTF, DOC ed ODT), Gnumeric come spreadsheet, la suite Seamonkey per la rete (web browser, mail client, editor HTML e client IRC) e l’efficiente ROX come file manager. E se volessimo Open Office o Firefox? Nessun problema, Puppy Linux fornisce un comodo sistema per l’installazione del software. Clickiamo sull’icona “install”: nella finestra che appare possiamo scegliere se installare i pacchetti aggiuntivi ufficiali (PET packages) o quelli non ufficiali (DotPup packages); si consiglia prima di cercare il software tra i pacchetti ufficiali, per poi in caso di necessità rivolgersi ai packages DotPup. Clickiamo quindi sull’icona “PETget package manager”, poi nella schermata successiva clickiamo sull’icona più grande presente in finestra. Apparirà una finestra in cui potremo selezionare i pacchetti che vogliamo installare, tutti perfettamente configurati per funzionare al meglio su Puppy Linux. Addirittura, una volta installato il software che ci serve potremo rimasterizzare il CD Live di Puppy Linux per avere una versione di questa distro con il nostro software preferito (Menu > Setup > Remaster Puppy live-CD)! ■



I programmi presenti in Puppy Linux non ci bastano? Installarne degli altri è di una semplicità disarmante!

LINK UTILI

http://www.puppylinux.org
http://puppylinux.org/wikka/PuppyLinuxMainPage

HACKERS MAGAZINE.IT

IN EDICOLA OGNI DUE MESI

TUTTI GLI STRUMENTI DEL VERO HACKER





Articoli di informazione, guide e consigli pratici!

La più grande raccolta di programmi per gli hacker è Hackers Magazine, 32 pagine sul filo del rasoio e software all'avanguardia

QUATTORD. ANNO 8 - N°147 - 20 MARZO/2 APRILE 2008 - € 2,00
WLF PUBLISHING